202004626

(19)中華民國智慧財產局

(12)發明說明書公開本 (11)公開編號：TW 202004626 A

(43)公開日： 中華民國 109 (2020) 年 01 月 16 日

(21)申請案號：107117106 (22)申請日： 中華民國 107 (2018) 年 05 月 18 日

(51)Int. Cl.： *G06Q40/00 (2012.01)*

(71)申請人：香港商泰德陽光有限公司 (香港地區) TIDETIME SUN LTD. (HK)
香港

(72)發明人：黃冠寰 HWANG, GWAN-HWAN (TW)

(74)代理人：劉光德

申請實體審查：有 申請專利範圍項數：39 項 圖式數：8 共 53 頁

(54)名稱

分散式金流稽核方法、裝置及系統

(57)摘要

本發明係一種分散式金流稽核方法、裝置及系統，該分散式金流稽核方法包括提供相關於使用者且儲存為第一索引模克樹的實體通貨兌換憑據或虛擬通貨之餘額資訊及相關於該餘額資訊且儲存為第二索引模克樹之交易的稽核資訊；以及該使用者比對該餘額資訊與該稽核資訊。該分散式金流稽核方法更包括該使用者與該中介者之間的溝通協定、該些使用者之間的證據協定及該第一索引模克樹與該第二索引模克樹之間所具有各階段完成時的清算協定。本發明能解決現有區塊鏈交易成本過高、公信力不佳及低效率等問題，並能支援實體通貨兌換憑據或虛擬通貨的一般性微支付。

指定代表圖：

符號簡單說明：

S10、S11・・・步驟

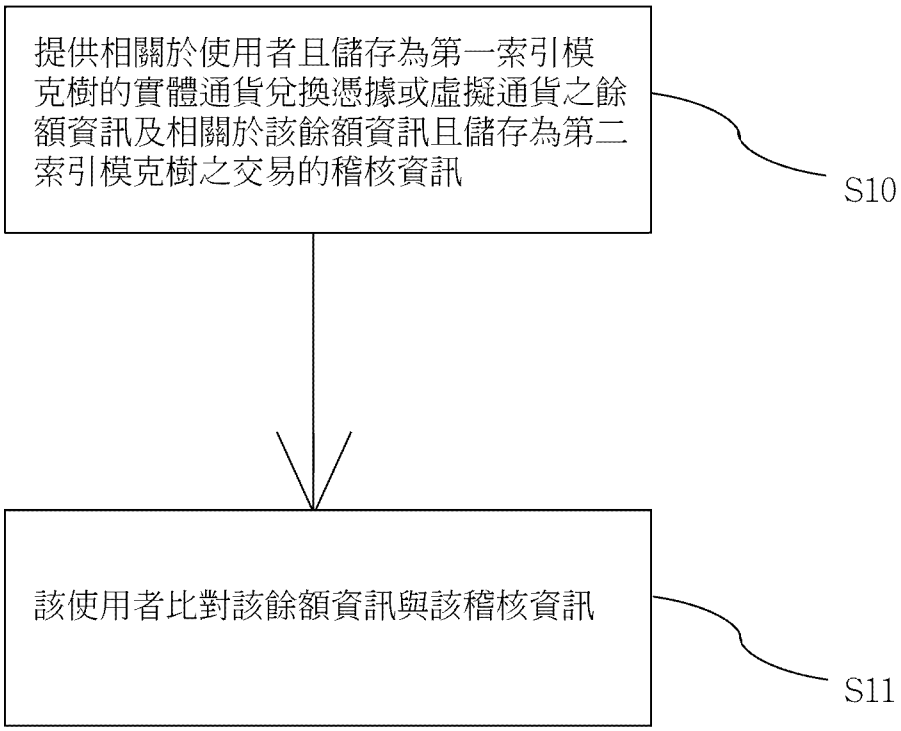

圖1

【發明說明書】

【中文發明名稱】　　分散式金流稽核方法、裝置及系統

【技術領域】

【0001】本發明是關於交易稽核之領域，更特定而言是關於分散式金流稽核方法、裝置及系統。

【先前技術】

【0002】在先前技術之區塊鏈實行中，由於單一筆金流交易之稽核資訊係以區塊鏈的礦工將交易儲存於區塊鏈中，現今公有區塊鏈的交易頻寬過低（每秒不超過25個）、同時因為區塊鏈的貨幣價值上漲，每筆金流交易的手續費成本過高。因此使用區塊鏈來進行一般性的微支付是不可行的。

【0003】所以一般採用區塊鏈下的交易，以加快金流交易的速度及降低交易成本。由於代理人負責向使用者收費，並紀錄及統計帳本，於每期間提供一對帳紀錄給權利人，告知本期間內，其交易紀錄，及對應之權利金等。惟，上述帳本係由代理人所紀錄及維護，權利人及/或使用者無從稽核其真實性。舉例而言，代理人可能非因故意，但系統有瑕疵而導致紀錄上有短缺或其他錯誤。亦或，代理人可能出於故意，刻意偽造或變造紀錄以減少應給付權利人之權利金。甚者，代理人可能宣稱某些下載量係不肖使用者利用破解等不正在權利人及/或使用者無從稽核其帳本真實性之下，除可能因此有損權利人及/或使用者之權益外，甚至可能降低權利人及/或使用者授權代理人代理交易之意願，對區塊鏈交易之發展亦非益事。

【0004】 有鑑於此，本發明提出一種分散式金流稽核方法、裝置及系統，以解決先前技術之區塊鏈實行中種種缺失，且能降低交易成本、提升交易公信力並達成低負擔及高效率，且能支援實體通貨兌換憑據或虛擬通貨的一般性微支付。

【發明內容】

【0005】 本發明提供一種分散式金流稽核方法，其包括提供相關於使用者且儲存為第一索引模克樹的實體通貨兌換憑據或虛擬通貨之餘額資訊及相關於該餘額資訊且儲存為第二索引模克樹之交易的稽核資訊；以及該使用者比對該餘額資訊與該稽核資訊。

【0006】 本發明之分散式金流稽核方法，其中，該稽核資訊係至少對應一合約。

【0007】 本發明之分散式金流稽核方法，其中，該使用者係與中介者以該合約而交易，且該中介者於該交易後更新該第一索引模克樹及該第二索引模克樹，於該使用者比對該餘額資訊與該稽核資訊異常時，產生證據資訊予該合約。

【0008】 本發明之分散式金流稽核方法，其中，該使用者與該中介者之間具有溝通協定，且在該使用者之數目為複數個時，該些使用者之間具有證據協定，在該交易之數目為複數個時，該中介者以一部分數目之該些交易作為一階段而更新該第一索引模克樹及該第二索引模克樹，且至少該第一索引模克樹與該第二索引模克樹之間具有各該階段完成時的清算協定。

【0009】 本發明之分散式金流稽核方法，其中，該使用者與該中介者之間具有溝通協定，且在該使用者之數目為複數個時，該些使用者之間具有證據協定，在該交易之數目為複數個時，該中介者以一部分數目之該些交易作為一階

段而更新該第一索引模克樹及該第二索引模克樹，且至少該第一索引模克樹與該第二索引模克樹之間具有各該階段完成時的清算協定。

【0010】本發明之分散式金流稽核方法，其中，該合約包含該中介者之抵押、該使用者之實體通貨兌換憑據或虛擬通貨、該使用者之實體通貨兌換憑據或虛擬通貨之儲金記錄、該合約與該第一索引模克樹及該第二索引模克樹之間的金流記錄、該些階段之序號、該第一索引模克樹及該第二索引模克樹之該些階段的雜湊值、以及該合約之函式。

【0011】本發明之分散式金流稽核方法，其中，該合約之函式包含將該使用者之實體通貨兌換憑據或該虛擬通貨存到該合約中的函式、將該使用者於該合約中的實體通貨兌換憑據或虛擬通貨轉移的函式、將該使用者於該合約中的實體通貨兌換憑據或虛擬通貨轉移至該第一索引模克樹的函式、將該第一索引模克樹之實體通貨兌換憑據或虛擬通貨的至少部分餘額轉移至該合約中的函式、結束一該階段並進行清算的函式、以及產生該證據資訊的函式。

【0012】本發明之分散式金流稽核方法，其中，該溝通協定包含轉帳交易、入金交易及出金交易。

【0013】本發明之分散式金流稽核方法，其中，該轉帳交易之步驟包含：該使用者送給該中介者T_{Rmit} = ((LSN, Remittance, Ui, Uj, X, 階段序號), $SIG_{Pri(Ui)}$)，LSN為該使用者產生的一不重複的亂數，$SIG_{Pri(Ui)}$為該使用者所簽署之訊息本體的電子簽章；該中介者將該第一索引模克樹中的不同使用者(Ui,Uj)之該實體通貨兌換憑據或虛擬通貨的餘額修改，假定Ui及Uj之該實體通貨兌換憑據或虛擬通貨的餘額於轉帳後分別為p,q；該中介者以T_{ACK} = ((T_{Rmit}, p, q, GSN), $SIG_{Pri(Agent)}$)回覆該使用者Ui， GSN為該中介者產生的一個整數，由0開始，每次處理一該使用者的交易後都會增加1予GSN，$SIG_{Pri(Agent)}$為該中介者所簽署之訊息本體的電子簽章；以及該中介者將T_{ACK}存到該第二索引模克樹。

【0014】本發明之分散式金流稽核方法，其中，該入金交易之步驟包含：該使用者(Ui)送給該中介者$T_{Deposit}$ = ((LSN, Deposit, X, 階段序號), $SIG_{Pri(Ui)}$)，LSN為該使用者產生的一不重複的亂數，$SIG_{Pri(Ui)}$為該使用者所簽署之訊息本體的電子簽章；該中介者將該第一索引模克樹中的使用者餘額修改，假定該使用者之實體通貨兌換憑據或虛擬通貨的餘額於轉帳後為p；該中介者令該合約中的Deposit_token_to_sidechain()執行，Deposit_token_to_sidechain()將該合約中的Ui.balance減去X，同時將該金流記錄增加一筆記錄：(Deposit, Ui, X, 階段序號, GSN)；該中介者以T_{ACK} = ((T_{Depost}, p, GSN), $SIG_{Pri(Agent)}$))回覆該使用者，GSN為該中介者產生的一由0開始之整數，每次處理一該使用者的交易後都會增加1予GSN，$SIG_{Pri(Agent)}$為該中介者所簽署之訊息本體的電子簽章；以及該中介者將T_{ACK}存到該第二索引模克樹。

【0015】本發明之分散式金流稽核方法，其中，該出金交易之步驟包含：該使用者(Ui)送給該中介者$T_{Withdraw}$ = ((LSN, Withdraw, X, 階段序號), $SIG_{Pri(Ui)}$)，LSN為該使用者產生的一不重複的亂數，$SIG_{Pri(Ui)}$為該使用者所簽署之訊息本體的電子簽章；該中介者修改該第一索引模克樹中該使用者之餘額，假定該使用者之實體通貨兌換憑據或虛擬通貨的餘額於轉帳後為p；該中介者令該合約中的Withdraw_token_from_sidechain()執行，Withdraw_token_from_sidechain()將該合約中的Ui.balance加上X，同時將該金流記錄增加一筆記錄：(Withdraw, Ui, X, 階段序號, GSN)；該中介者以T_{ACK} = (($T_{Withdraw}$, p, GSN), $SIG_{Pri(Agent)}$) 回覆該使用者，GSN為該中介者產生的一由0開始之整數，每次處理一該使用者的交易後都會增加1予GSN，$SIG_{Pri(Agent)}$為該中介者所簽署之訊息本體的電子簽章；以及該中介者將T_{ACK}存到該第二索引模克樹。

【0016】本發明之分散式金流稽核方法，其中，該合約更包含函式Finalize()，該中介者執行Finalize()以將該第一索引模克樹及該第二索引模克樹於現有階段結束後的雜湊值儲存於該合約並公布，同時該中介者公布該現有階段結束後的至少部分該第一索引模克樹及至少部分該第二索引模克樹以供查詢。

【0017】本發明之分散式金流稽核方法，其中，該合約具有函式Fraud_proof()以產生該證據資訊，產生該證據資訊係於以下情況或其組合產生：（1）該中介者於處理轉帳交易、入金交易或出金交易後沒有將交易儲存於該第二索引模克樹，該使用者執行Fraud_proof()函式以提出由該中介者回傳的T_{ACK}及該第二索引模克樹的切片，證明該中介者沒有將該交易儲存於該第二索引模克樹；（2）該中介者於處理該轉帳交易、該入金交易或該出金交易後將該使用者的餘額算錯，由於該中介者每個交易之回傳的T_{ACK}都有GSN，其數值為遞增且不重複，故該使用者將該交易排序並找出發生錯誤交易的前一個交易的該中介者之回傳T_{ACK}，之後該使用者執行Fraud_proof()函式，將此錯誤交易及前一個交易的該中介者之回傳T_{ACK}為證據，而證明該中介者提不出有GSN值介於此兩交易中GSN值的交易以證明該中介者出錯。

【0018】本發明之分散式金流稽核方法，其中，該第一索引模克樹及該第二索引模克樹係對應一區塊鏈。

【0019】本發明提供一種分散式金流稽核裝置，其包括處理單元及儲存單元，該處理單元產生相關於使用者且為實體通貨兌換憑據或虛擬通貨之餘額資訊的第一索引模克樹，以及產生相關於該餘額資訊之交易的稽核資訊之第二索引模克樹，且比對該餘額資訊與該稽核資訊，以及該儲存單元耦接該處理單元，儲存該第一索引模克樹及該第二索引模克樹。

【0020】本發明之分散式金流稽核裝置，其中，該稽核資訊係至少對應一合約，且該處理單元處理該合約，該儲存單元儲存該合約。

【0021】本發明之分散式金流稽核裝置，其中，該使用者與中介者係以該合約而交易，且該中介者於交易後令該處理單元更新該第一索引模克樹及該第二索引模克樹，於該使用者令該處理單元比對該餘額資訊與該稽核資訊異常時，該處理單元產生證據資訊予該合約，該儲存單元儲存該證據資訊。

【0022】本發明之分散式金流稽核裝置，其中，該使用者與該中介者之間具有溝通協定，且在該使用者之數目為複數個時，該些使用者之間具有證據協定，該處理單元處理該溝通協定及該證據協定，且該儲存單元儲存該溝通協定及該證據協定，在該交易之數目為複數個時，該中介者以一部分數目之該些交易作為一階段而令該處理單元更新該第一索引模克樹及該第二索引模克樹，該儲存單元儲存更新之該第一索引模克樹及該第二索引模克樹，且至少該第一索引模克樹與該第二索引模克樹之間具有各該階段完成時的清算協定，該處理單元處理該清算協定且該儲存單元儲存該清算協定。

【0023】本發明之分散式金流稽核裝置，其中，該合約包含該中介者之抵押、該使用者之實體通貨兌換憑據或虛擬通貨、該使用者之實體通貨兌換憑據或虛擬通貨之儲金記錄、該合約與該第一索引模克樹及該第二索引模克樹之間的金流記錄、該些階段之序號、該第一索引模克樹及該第二索引模克樹之該些階段的雜湊值、以及該合約之函式。

【0024】本發明之分散式金流稽核裝置，其中，該合約之函式包含將該使用者之實體通貨兌換憑據或該虛擬通貨存到該合約中的函式、將該使用者於該合約中的實體通貨兌換憑據或虛擬通貨轉移的函式、將該使用者於該合約中的實體通貨兌換憑據或虛擬通貨轉移至該第一索引模克樹的函式、將該第一索引

模克樹之實體通貨兌換憑據或虛擬通貨的至少部分餘額轉移至該合約中的函式、結束一該階段並進行清算的函式、以及產生該證據資訊的函式。

【0025】本發明之分散式金流稽核裝置，其中，該溝通協定包含轉帳交易、入金交易及出金交易。

【0026】本發明之分散式金流稽核裝置，其中，該轉帳交易之步驟包含：該使用者令該處理單元送給該中介者T_{Rmit} = ((LSN, Remittance, Ui, Uj, X, 階段序號), $SIG_{Pri(Ui)}$)，LSN為該使用者產生的一不重複的亂數，$SIG_{Pri(Ui)}$為該使用者所簽署之訊息本體的電子簽章；該中介者令該處理單元將該第一索引模克樹中的不同使用者(Ui,Uj)之該實體通貨兌換憑據或虛擬通貨的餘額修改，假定Ui及Uj之該實體通貨兌換憑據或虛擬通貨的餘額於轉帳後分別為p,q；該中介者令該處理單元以T_{ACK} = ((T_{Rmit}, p, q, GSN), $SIG_{Pri(Agent)}$)回覆該使用者Ui，GSN為該中介者產生的一個整數，由0開始，該處理單元每次處理一該使用者的交易後都會增加1予GSN，$SIG_{Pri(Agent)}$為該中介者所簽署之訊息本體的電子簽章；以及該中介者令該處理單元將T_{ACK}存到該第二索引模克樹。

【0027】本發明之分散式金流稽核裝置，其中，該入金交易之步驟包含：該使用者(Ui)令該處理單元送給該中介者$T_{Deposit}$ = ((LSN, Deposit, X, 階段序號), $SIG_{Pri(Ui)}$)，LSN為該使用者產生的一不重複的亂數，$SIG_{Pri(Ui)}$為該使用者所簽署之訊息本體的電子簽章；該中介者令該處理單元將該第一索引模克樹中的使用者餘額修改，假定該使用者之實體通貨兌換憑據或虛擬通貨的餘額於轉帳後為p；該中介者令該處理單元執行該合約中的Deposit_token_to_sidechain()，Deposit_token_to_sidechain()將該合約中的Ui.balance減去X，同時將該金流記錄增加一筆記錄：(Deposit, Ui, X, 階段序號, GSN)；該中介者令該處理單元以T_{ACK} = ((T_{Depost}, p, GSN), $SIG_{Pri(Agent)}$))回覆該使用者，GSN為該中介者產生的一由0開始之整數，該處理單元每次處理一該使用者的交易後都會增加1予

GSN，$SIG_{Pri(Agent)}$為該中介者所簽署之訊息本體的電子簽章；以及該中介者令該處理單元將T_{ACK}存到該第二索引模克樹。

【0028】本發明之分散式金流稽核裝置，其中，該出金交易之步驟包含：該使用者(Ui)令該處理單元送給該中介者$T_{Withdraw}$ = ((LSN, Withdraw, X, 階段序號), $SIG_{Pri(Ui)}$)，LSN為該使用者產生的一不重複的亂數，$SIG_{Pri(Ui)}$為該使用者所簽署之訊息本體的電子簽章；該中介者令該處理單元修改該第一索引模克樹中該使用者之餘額，假定該使用者之實體通貨兌換憑據或虛擬通貨的餘額於轉帳後為p；該中介者令該處理單元執行該合約中的Withdraw_token_from_sidechain()，Withdraw_token_from_sidechain()將該合約中的Ui.balance加上X，同時將該金流記錄增加一筆記錄：(Withdraw, Ui, X, 階段序號, GSN)；該中介者令該處理單元以T_{ACK} = (($T_{Withdraw}$, p, GSN), $SIG_{Pri(Agent)}$) 回覆該使用者，GSN為該中介者產生的一由0開始之整數，該處理單元每次處理一該使用者的交易後都會增加1予GSN，$SIG_{Pri(Agent)}$為該中介者所簽署之訊息本體的電子簽章；以及該中介者令該處理單元將T_{ACK}存到該第二索引模克樹。

【0029】本發明之分散式金流稽核裝置，其中，該合約更包含函式Finalize()，該中介者令該處理單元執行Finalize()以將該第一索引模克樹及該第二索引模克樹於現有階段結束後的雜湊值儲存於該合約並公布，同時該中介者公布該現有階段結束後的至少部分該第一索引模克樹及至少部分該第二索引模克樹以供查詢。

【0030】本發明之分散式金流稽核裝置，其中，該合約具有函式Fraud_proof()以產生該證據資訊，產生該證據資訊係於以下情況或其組合產生：（1）該中介者於該處理單元處理轉帳交易、入金交易或出金交易後沒有將交易儲存於該第二索引模克樹，該使用者令該處理單元執行Fraud_proof()函式

以提出由該中介者回傳的T_{ACK}及該第二索引模克樹的切片，證明該中介者沒有將該交易儲存於該第二索引模克樹；（2）該中介者於該處理單元處理該轉帳交易、該入金交易或該出金交易後將該使用者的餘額算錯，由於該中介者每個交易之回傳的T_{ACK}都有GSN，GSN之數值為遞增且不重複，故該使用者令該處理單元將該交易排序並找出發生錯誤交易的前一個交易的該中介者之回傳T_{ACK}，之後該使用者令該處理單元執行Fraud_proof()函式，將此錯誤交易及前一個交易的該中介者之回傳T_{ACK}為證據，而證明該中介者提不出有GSN值介於此兩交易中GSN值的交易以證明該中介者出錯。

【0031】本發明之分散式金流稽核裝置，其中，該第一索引模克樹及該第二索引模克樹係對應一區塊鏈。本發明提供一種分散式金流稽核系統，其包括複數個金流稽核裝置，其至少一者係包含處理單元或儲存單元，且該些金流稽核裝置具有資料傳輸單元，至少一該處理單元產生相關於使用者且為實體通貨兌換憑據或虛擬通貨之餘額資訊的第一索引模克樹、產生相關於該餘額資訊之交易的稽核資訊之第二索引模克樹、比對該餘額資訊與該稽核資訊或其組合，該資料傳輸單元傳輸至少部分對應該第一索引模克樹之資訊、至少部分對應該第二索引模克樹之資訊、該餘額資訊與該稽核資訊之比對結果或其組合，該儲存單元耦接該處理單元或該資料傳輸單元，以儲存該第一索引模克樹或該第二索引模克樹。

【0032】本發明之分散式金流稽核系統，其中，該稽核資訊係至少對應一合約，且至少一該處理單元處理該合約，至少一該儲存單元儲存該合約。

【0033】本發明之分散式金流稽核系統，其中，該使用者係與中介者以該合約而交易，且該中介者於交易後令至少一該處理單元更新該第一索引模克樹及該第二索引模克樹，於該使用者令至少一該處理單元比對該餘額資訊與該稽

核資訊異常時，至少一該處理單元產生證據資訊予該合約，且至少一該儲存單元儲存該證據資訊。

【0034】本發明之分散式金流稽核系統，其中，該使用者與該中介者之間具有溝通協定，且在該使用者之數目為複數個時，該些使用者之間具有證據協定，至少一該處理單元處理該溝通協定及該證據協定，且至少一該儲存單元儲存該溝通協定及該證據協定，在該交易之數目為複數個時，該中介者以一部分數目之該些交易作為一階段而令至少一該處理單元更新該第一索引模克樹及該第二索引模克樹，至少一該儲存單元儲存更新之該第一索引模克樹及該第二索引模克樹，且至少該第一索引模克樹與該第二索引模克樹之間具有各該階段完成時的清算協定，至少一該處理單元處理該清算協定且至少一該儲存單元儲存該清算協定。

【0035】本發明之分散式金流稽核系統，其中，該合約包含該中介者之抵押、該使用者之實體通貨兌換憑據或虛擬通貨、該使用者之實體通貨兌換憑據或虛擬通貨之儲金記錄、該合約與該第一索引模克樹及該第二索引模克樹之間的金流記錄、該些階段之序號、該第一索引模克樹及該第二索引模克樹之該些階段的雜湊值、以及該合約之函式。

【0036】本發明之分散式金流稽核系統，其中，該合約之函式包含將該使用者之實體通貨兌換憑據或該虛擬通貨存到該合約中的函式、將該使用者於該合約中的實體通貨兌換憑據或虛擬通貨轉移的函式、將該使用者於該合約中的實體通貨兌換憑據或虛擬通貨轉移至該第一索引模克樹的函式、將該第一索引模克樹之實體通貨兌換憑據或虛擬通貨的至少部分餘額轉移至該合約中的函式、結束一該階段並進行清算的函式、以及產生該證據資訊的函式。

【0037】本發明之分散式金流稽核系統，其中，該溝通協定包含轉帳交易、入金交易及出金交易。

【0038】本發明之分散式金流稽核系統，其中，該轉帳交易之步驟包含：該使用者令至少一該處理單元送給該中介者T_{Rmit} = ((LSN, Remittance, Ui, Uj, X, 階段序號), $SIG_{Pri(Ui)}$)，LSN為該使用者產生的一不重複的亂數，$SIG_{Pri(Ui)}$為該使用者所簽署之訊息本體的電子簽章；該中介者令至少一該處理單元將該第一索引模克樹中的不同使用者(Ui,Uj)之該實體通貨兌換憑據或虛擬通貨的餘額修改，假定Ui及Uj之該實體通貨兌換憑據或虛擬通貨的餘額於轉帳後分別為p,q；該中介者令至少一該處理單元以T_{ACK} = ((T_{Rmit}, p, q, GSN), $SIG_{Pri(Agent)}$)回覆該使用者Ui，GSN為該中介者產生的一個整數，由0開始，至少一該處理單元每次處理一該使用者的交易後都會增加1予GSN，$SIG_{Pri(Agent)}$為該中介者所簽署之訊息本體的電子簽章；以及該中介者令至少一該處理單元將T_{ACK}存到該第二索引模克樹。

【0039】本發明之分散式金流稽核系統，其中，該入金交易之步驟包含：該使用者(Ui)令至少一該處理單元送給該中介者$T_{Deposit}$ = ((LSN, Deposit, X, 階段序號), $SIG_{Pri(Ui)}$)， LSN為該使用者產生的一不重複的亂數，$SIG_{Pri(Ui)}$為該使用者所簽署之訊息本體的電子簽章；該中介者令至少一該處理單元將該第一索引模克樹中的使用者餘額修改，假定該使用者之實體通貨兌換憑據或虛擬通貨的餘額於轉帳後為p；該中介者令至少一該處理單元執行該合約中的Deposit_token_to_sidechain()，Deposit_token_to_sidechain()將該合約中的Ui.balance減去X，同時將該金流記錄增加一筆記錄：(Deposit, Ui, X, 階段序號, GSN)；該中介者令至少一該處理單元以T_{ACK} = ((T_{Depost}, p, GSN), $SIG_{Pri(Agent)}$))回覆該使用者，GSN為該中介者產生的一由0開始之整數，至少一該處理單元每次處理一該使用者的交易後都會增加1予GSN，$SIG_{Pri(Agent)}$為該中介者所簽署之訊息本體的電子簽章；以及該中介者令至少一該處理單元將T_{ACK}存到該第二索引模克樹。

【0040】本發明之分散式金流稽核系統，其中，該合約更包含函式Finalize()，該中介者令至少一該處理單元執行Finalize()以將該第一索引模克樹及該第二索引模克樹於現有階段結束後的雜湊值儲存於該合約並公布，同時該中介者公布該現有階段結束後的至少部分該第一索引模克樹及至少部分該第二索引模克樹以供查詢。

【0041】本發明之分散式金流稽核系統，其中，該合約具有函式Fraud_proof()以產生該證據資訊，產生該證據資訊係於以下情況或其組合產生：（1）該中介者於至少一該處理單元處理轉帳交易、入金交易或出金交易後沒有將交易儲存於該第二索引模克樹，該使用者令至少一該處理單元執行Fraud_proof()函式以提出由該中介者回傳的T_{ACK}及該第二索引模克樹的切片，證明該中介者沒有將該交易儲存於該第二索引模克樹；（2）該中介者於至少一該處理單元處理該轉帳交易、該入金交易或該出金交易後將該使用者的餘額算錯，由於該中介者每個交易之回傳的T_{ACK}都有GSN，GSN之數值為遞增且不重複，故該使用者令至少一該處理單元將該交易排序並找出發生錯誤交易的前一個交易的該中介者之回傳T_{ACK}，之後該使用者令至少一該處理單元執行Fraud_proof()函式，將此錯誤交易及前一個交易的該中介者之回傳T_{ACK}為證據，而證明該中介者提不出有GSN值介於此兩交易中GSN值的交易以證明該中介者出錯。

【0042】本發明之分散式金流稽核系統，更包括區塊鏈裝置或區塊鏈單元，該區塊鏈裝置與至少一該金流稽核裝置耦接，該區塊鏈單元設置於至少一該金流稽核裝置，該第一索引模克樹及該第二索引模克樹係至少對應該區塊鏈裝置或該區塊鏈單元中之一區塊鏈。

【0043】相較於習知技術，本發明能節省傳輸稽核資訊之時間、次數、手續費等成本。另外，本發明能提升交易之公信力。再者，本發明能達成低負擔

且高效率之系統。並且，本發明能支援實體通貨兌換憑據或虛擬通貨的一般性微支付。

【圖式簡單說明】

【0044】 圖1係本發明分散式金流稽核方法之流程圖。

圖2係切片之示意圖。

圖3係本發明之合約內容的方塊圖。

圖4係本發明之轉帳交易的流程圖。

圖5係本發明之入金交易的流程圖。

圖6係本發明之出金交易的流程圖。

圖7係本發明之一種分散式金流稽核裝置的方塊圖。

圖7係本發明之一種分散式金流稽核系統的方塊圖。

【實施方式】

【0045】 為充分瞭解本發明之目的、特徵及功效，茲藉由下述具體之實施例，並配合所附之圖式，對本發明做一詳細說明，說明如後：

【0046】 請參考圖1，係本發明分散式金流稽核方法之流程圖，其步驟包括步驟S10至步驟S11。步驟S10中，其可提供相關於使用者且儲存為第一索引模克樹的實體通貨兌換憑據或虛擬通貨之餘額資訊及相關於該餘額資訊且儲存為第二索引模克樹之交易的稽核資訊。其中，第一索引模克樹及第二索引模克樹可為完滿二元雜湊樹(Full Hash Binary Tree)與指標函數 Γ(Index function, 即 $\Gamma(\text{FileName})=\text{SHA-256}(\text{FileName}) \bmod 2^{N-1}$) 之結合。惟於其他實施例中，並不限於利用其他雜湊樹。該稽核資訊可相關於使用者，特定而言，可為複數個使用者。其中，該稽核資訊譬如一帳本，紀錄使用者之交易紀錄。於不同實施例中，

使用者之數量可能相當龐大，譬如應用於有五十萬使用者之加密貨幣應用、商品或勞務交易平台等。實體通貨兌換憑據可例如為實體通貨之存摺、票據、股票、地契、電子錢包等，而虛擬通貨可例如為比特幣、以太幣等，惟本發明不限於此。再者，該稽核資訊可為複數筆交易之累積稽核資訊，從而節省傳輸稽核資訊之時間、次數、手續費等成本。特定而言，本發明之該第一索引模克樹及該第二索引模克樹可對應一區塊鏈。該使用者可為交易者、區塊鏈之參與者或其它參與者。

【0047】另外，可藉由雜湊函數而根據該稽核資訊作成一濃縮狀態碼。雜湊函數可利用「MD5」、「RIPEMD160」、「SHA1」、「SHA256」、「SHA384」、「SHA512」或其他雜湊函數。較佳實施例中可利用SHA系列雜湊函數，且更特定而言可利用「SHA256」雜湊函數。藉此，濃縮狀態碼可用來檢驗該稽核資訊之完整性及同一性，且具有不可逆性質，無法反向導出原始資料。再者，經過濃縮，有壓縮檔案大小之效果，以便利傳輸。

【0048】該第一索引模克樹可包含第一切片(Slice)且該第二索引模克樹可包含第二切片，詳細而言該稽核資訊可作成複數個切片，參考圖2，其繪示切片之示意圖。可表示為取出特定部分之雜湊樹。藉此，本發明可根據該使用者作成與該使用者相關之切片。因此，藉由各切片，該使用者僅得審閱關於自己的交易資訊。另外，該稽核資訊可至少對應一合約。舉例而言，該合約可為以太坊的智能合約，惟本發明不限於此。

【0049】步驟S11中，該使用者可比對該餘額資訊與該稽核資訊。在該使用者初入金時，本發明之分散式金流稽核方法可僅比對初入金之該餘額資訊與該稽核資訊。特定而言，比對該餘額資訊與該稽核資訊可比對該第一切片與該第二切片。另外，該使用者可與中介者以該合約而交易，且該中介者更新該第一索引模克樹及該第二索引模克樹，於該使用者比對該餘額資訊與該稽核資訊異

常時，產生證據(Fraud Proof)資訊予該合約。該中介者可為代理人、仲介、管理者等。

【0050】詳細而言，可將該濃縮狀態碼及相關於該使用者之交易的切片一起送予該使用者，因此該使用者可藉由該濃縮狀態碼確認其切片具有同一性，進而比對該使用者之交易資訊(帳本)是否正確，以決定是否作出錯誤回報。藉此，雖然該使用者皆僅利用各切片，而僅比對關於自身的交易資訊是否正確，惟因為本發明實施例中，利用該濃縮狀態碼，使各切片與該稽核資訊之間具有同一性，或稱唯一性，而具有綁定之效果。因此，只要該使用者作出錯誤回報，就可比對出該稽核資訊為不正確。亦即，將比對之工作分散於該使用者。且讓該使用者在檢視自己之交易資訊時，無形中幫忙做了比對之工作，而並未增加該使用者之負擔。且於較佳實施例中，該濃縮狀態碼及其切片之確認動作，可利用該使用者之應用程式自動進行。

【0051】在本發明實施例中，利用該濃縮狀態碼及切片，可大幅縮減需要傳輸之資料量。舉例而言，在一實施例中，若有50萬個使用者，則設置雜湊樹所需記憶體空間約為206.9百萬位元組(Megabyte，MB)，而該使用者接收該濃縮狀態碼僅需下載約32位元組(Byte，B)、接收切片僅需下載1千位元組(KB)。下載量僅占原始帳本(稽核資訊)之約十萬分之一，且理想狀態下，比對僅須費時約千分之一秒。可適用於具有大量使用者之加密貨幣應用、商品或勞務交易平台等，而不會有明顯延遲感等不佳使用者體驗。達成低負擔且高效率之系統。另外，由於本發明實施例中該中介者可提供一筆抵押，例如該實體通貨兌換憑據或虛擬通貨，予該合約，故於該使用者比對該餘額資訊與該稽核資訊異常並產生證據資訊予該合約後，可由該抵押支付賠償予該使用者，從而提升本發明之公信力。

【0052】進一步而言，本發明之分散式金流稽核方法的該使用者與該中介者之間具有溝通協定，且在該使用者之數目為複數個時，該些使用者之間具有證據協定，在該交易之數目為複數個時，該中介者以一部分數目之該些交易作為一階段而更新該第一索引模克樹及該第二索引模克樹，且至少該第一索引模克樹與該第二索引模克樹之間具有各該階段完成時的清算協定。而該溝通協定可包含轉帳交易、入金交易及出金交易。因此，本發明可以該些協定而建立複數個使用者之間及使用者與至少一個中介者之間的多對多交易管道以支援實體通貨兌換憑據或虛擬通貨的一般性微支付。

【0053】詳細而言並請參閱圖3，該合約可包含該中介者之抵押、該使用者之實體通貨兌換憑據或虛擬通貨、該使用者之實體通貨兌換憑據或虛擬通貨之儲金記錄、該合約與該第一索引模克樹及該第二索引模克樹之間的金流記錄、該些階段之序號、該第一索引模克樹及該第二索引模克樹之該些階段的雜湊值、以及該合約之函式。

【0054】如上所述之該合約之函式可包含將該使用者之實體通貨兌換憑據或該虛擬通貨存到該合約中的函式(即Transfer_token_to_contact()，特定而言為金流交易人擁有的虛擬通貨存到智能合約中)、將該使用者於該合約中的實體通貨兌換憑據或虛擬通貨轉移的函式(即Transfer_token_out()，特定而言為金流交易人將自己在此合約中的虛擬通貨轉到區塊鏈其他帳戶中)、將該使用者於該合約中的實體通貨兌換憑據或虛擬通貨轉移至該第一索引模克樹的函式(即Deposit_token_to_sidechain()，特定而言為將金流交易人在合約中的虛擬通貨轉移到第一索引模克樹)、將該第一索引模克樹之實體通貨兌換憑據或虛擬通貨的至少部分餘額轉移至該合約中的函式(即Withdraw_token_from_sidechain()，特定而言為將第一索引模克樹的虛擬通貨餘額轉到智能合約中)、結束一該階段

並進行清算的函式(即Finalize()，特定而言為結束一個階段，進行清算)、以及產生該證據資訊的函式(即Fraud_Proof())，惟本發明不限於此。

【0055】 請參閱圖4，如上所述之轉帳交易(例如交易人Ui要將X單位的虛擬通貨轉帳給Uj)之步驟可包含以下步驟：步驟S401至步驟S404。步驟S401中，該使用者送給該中介者T_{Rmit} = ((LSN, Remittance, Ui, Uj, X, 階段序號), $SIG_{Pri(Ui)}$)，LSN為該使用者產生的一不重複的亂數，$SIG_{Pri(Ui)}$為該使用者所簽署之訊息本體的電子簽章。特定而言，參與交易人Ui首先送給代理人訊息T_{Rmit} = ((LSN, Remittance, Ui, Uj, X, 階段序號), $SIG_{Pri(Ui)}$)，其中LSN（Local sequence number）為交易人Ui產生的一個不會重複的亂數，$SIG_{Pri(Ui)}$為由Ui所簽署之訊息本體的電子簽章。步驟S402中，該中介者將該第一索引模克樹中的不同使用者(Ui,Uj)之該實體通貨兌換憑據或虛擬通貨的餘額修改，假定Ui及Uj之該實體通貨兌換憑據或虛擬通貨的餘額於轉帳後分別為p,q。特定而言，代理人將第一索引模克樹的中交易人Ui及Uj的虛擬通貨的餘額修改，假定Ui及Uj的虛擬通貨的餘額於轉帳後分別為p、q。步驟S403中，該中介者以T_{ACK} = ((T_{Rmit}, p, q, GSN), $SIG_{Pri(Agent)}$)回覆該使用者Ui， GSN為該中介者產生的一個整數，由0開始，每次處理一該使用者的交易後都會增加1予GSN，$SIG_{Pri(Agent)}$為該中介者所簽署之訊息本體的電子簽章。特定而言，代理人回覆交易人Ui訊息T_{ACK} = ((T_{Rmit}, p, q, GSN), $SIG_{Pri(Agent)}$)，其中GSN（Global sequence number(廣域序列數)）為代理人產生的一個整數，由0開始，每次處理一個交易人的交易後都會增加1。$SIG_{Pri(Agent)}$為由中介者所簽署之訊息本體的電子簽章。步驟S404中，該中介者將T_{ACK}存到該第二索引模克樹。

【0056】 請參閱圖5，如上所述之入金交易(例如交易人Ui要將智能合約X單位的虛擬通貨轉移到第一索引模克樹)之步驟可包含以下步驟：步驟S501至步驟S505。步驟S501中，該使用者(Ui)送給該中介者$T_{Deposit}$ = ((LSN, Deposit, X, 階

段序號), $SIG_{Pri(Ui)}$)， LSN為該使用者產生的一不重複的亂數，$SIG_{Pri(Ui)}$為該使用者所簽署之訊息本體的電子簽章。特定而言，參與交易人Ui首先送給代理人訊息$T_{Deposit}$ = ((LSN, Deposit, X, 階段序號), $SIG_{Pri(Ui)}$)，其中LSN (Local sequence number) 為交易人Ui產生的一個不會重複的亂數，$SIG_{Pri(Ui)}$為由Ui所簽署之訊息本體的電子簽章。步驟S502中，該中介者將該第一索引模克樹中的使用者餘額修改，假定該使用者之實體通貨兌換憑據或虛擬通貨的餘額於轉帳後為p。特定而言，代理人將第一索引模克樹中的交易人Ui餘額修改(增加X)，假定Ui於轉帳後分別為p。步驟S503中，該中介者令該合約中的Deposit_token_to_sidechain()執行，Deposit_token_to_sidechain()將該合約中的Ui.balance減去X，同時將該金流記錄增加一筆記錄：(Deposit, Ui, X, 階段序號, GSN) 。特定而言，代理人呼叫執行智能合約中的Deposit_token_to_sidechain()，此函式會將合約中的Ui.balance減去X，同時將合約及側鏈間的金流記錄增加一筆記錄 : (Deposit, Ui, X, 階段序號, GSN)。步驟S504中，該中介者以T_{ACK} = ((T_{Depost}, p, GSN), $SIG_{Pri(Agent)}$))回覆該使用者，GSN為該中介者產生的一由0開始之整數，每次處理一該使用者的交易後都會增加1予GSN，$SIG_{Pri(Agent)}$為該中介者所簽署之訊息本體的電子簽章。特定而言，代理人回覆交易人Ui訊息T_{ACK} = ((T_{Depost}, p, GSN), $SIG_{Pri(Agent)}$)，其中GSN為代理人產生的一個整數，由0開始，每次處理一個交易人的交易後都會增加1。$SIG_{Pri(Agent)}$為由中介者所簽署之訊息本體的電子簽章。步驟S505中，該中介者將T_{ACK}存到該第二索引模克樹。

【0057】 請參閱圖6，如上所述之出金交易(例如交易人Ui要將第一個索引模克樹的虛擬通貨X單位轉移到智能合約)之步驟可包含以下步驟：步驟S601至步驟S605。步驟S601中，該使用者(Ui)送給該中介者$T_{Withdraw}$ = ((LSN, Withdraw, X, 階段序號), $SIG_{Pri(Ui)}$)，LSN為該使用者產生的一不重複的亂數，$SIG_{Pri(Ui)}$為該使用者所簽署之訊息本體的電子簽章。特定而言，參與交易人Ui送給代理人訊

息$T_{Withdraw}$ = ((LSN, Withdraw, X, 階段序號), $SIG_{Pri(Ui)}$)，其中LSN（Local sequence number）為交易人Ui產生的一個不會重複的亂數，$SIG_{Pri(Ui)}$為由Ui所簽署之訊息本體的電子簽章。步驟S602中，該中介者修改該第一索引模克樹中該使用者之餘額，假定該使用者之實體通貨兌換憑據或虛擬通貨的餘額於轉帳後為p。特定而言，代理人將第一索引模克樹中的交易人Ui餘額修改(減去X)，假定Ui於轉帳後分別為p。步驟S603中，該中介者令該合約中的Withdraw_token_from_sidechain()執行，Withdraw_token_from_sidechain()將該合約中的Ui.balance加上X，同時將該金流記錄增加一筆記錄。特定而言，代理人呼叫執行智能合約中的Withdraw_token_from_sidechain()，此函式會將合約中的Ui.balance加上X，同時將合約及側鏈(第一及/或第二索引模克樹)間的金流記錄增加一筆記錄：(Withdraw, Ui, X, 階段序號, GSN)。步驟S604中，該中介者以T_{ACK} = (($T_{Withdraw}$, p, GSN), $SIG_{Pri(Agent)}$) 回覆該使用者，GSN為該中介者產生的一由0開始之整數，每次處理一該使用者的交易後都會增加1予GSN，$SIG_{Pri(Agent)}$為該中介者所簽署之訊息本體的電子簽章。特定而言，代理人回覆交易人Ui訊息T_{ACK} = (($T_{Withdraw}$, p, GSN), $SIG_{Pri(Agent)}$)，其中GSN為代理人產生的一個整數，由0開始，每次處理一個交易人的交易後都會增加1，且$SIG_{Pri(Agent)}$為由中介者所簽署之訊息本體的電子簽章。步驟S605中，該中介者將T_{ACK}存到該第二索引模克樹。

【0058】進一步而言，該中介者更新該第一索引模克樹及該第二索引模克樹可包含產生對應該第一索引模克樹之第一根雜湊值(Root Hash)及對應該第二索引模克樹之第二根雜湊值，且該中介者以該第一根雜湊值及該第二根雜湊值更新該合約。

【0059】另外，該合約更包含函式Finalize()，其中該中介者執行Finalize()以將該第一索引模克樹及該第二索引模克樹於現有階段結束後的雜湊值儲存於

該合約並公布，同時該中介者公布該現有階段結束後的至少部分該第一索引模克樹及至少部分該第二索引模克樹以供查詢。特定而言，智能合約中的函式Finalize()為代理人於約定的時間到期後，進行運作的清算協定。因此，本發明之一種分散式金流稽核方法可將一段時間內的交易整合清算以節省傳輸稽核資訊之時間、次數、手續費等成本。而代理人執行此函式，以將第一索引模克樹及第二索引模克樹於現有階段結束後的雜湊值儲存於合約以公布之。同時代理人亦公布階段結束後的至少部分第一索引模克樹及至少部分第二索引模克樹供查詢。

【0060】再者，該合約可具有函式Fraud_proof()以產生該證據資訊，該證據資訊可於以下情況或其組合產生：（1）該中介者於處理轉帳交易、入金交易或出金交易後沒有將交易儲存於該第二索引模克樹，該使用者執行Fraud_proof()函式以提出由該中介者回傳的T_{ACK}及該第二索引模克樹的切片，證明該中介者沒有將該交易儲存於該第二索引模克樹；（2）該中介者於處理該轉帳交易、該入金交易或該出金交易後將該使用者的餘額算錯，由於該中介者每個交易之回傳的T_{ACK}都有GSN，其數值為遞增且不重複，故該使用者將該交易排序並找出發生錯誤交易的前一個交易的該中介者之回傳T_{ACK}，之後該使用者執行Fraud_proof()函式，將此錯誤交易及前一個交易的該中介者之回傳T_{ACK}為證據，而證明該中介者提不出有GSN值介於此兩交易中GSN值的交易以證明該中介者出錯。特定而言，智能合約中的函式Fraud_proof()可以由交易人或其他參與者提出密碼學證據來證明代理人有發生錯誤。既有以下的可能情形：（1）代理人於處理轉帳交易、入金交易、出金交易後並沒有將交易儲存於第二索引模克樹：交易人或其他參與者可以執行Fraud_proof()函式，提出由代理人回傳的T_{ACK}及第二索引模克樹的切片，來證明代理人沒有將交易儲存於第二索引模克樹；（2）代理人於處理轉帳交易、入金交易、出金交易後將交易人的餘額算

錯：因為代理人每個交易的回傳訊息T_{ACK}都有GSN，其數值必須為遞增且不得重複，所以交易人可以將自己的交易排序，找出發生錯誤交易的前一個交易的代理人回傳交易訊息，執行Fraud_proof()函式，將此錯誤交易及前一個交易的回傳交易訊息為證據，因為代理人提不出有GSN值介於此兩交易中GSN值的交易，所以可以證明代理人出錯。

【0061】如圖7所示，其係本發明之一種分散式金流稽核裝置7的方塊圖，其可包括處理單元71及儲存單元72。如上所述之處理單元71可產生相關於使用者且為實體通貨兌換憑據或虛擬通貨之餘額資訊的第一索引模克樹，以及產生相關於該餘額資訊之交易的稽核資訊之第二索引模克樹，且比對該餘額資訊與該稽核資訊。處理單元71可為電路、晶片、中央處理器、微處理器(MCU)或其組合，惟本發明不限於此。

【0062】如上所述之儲存單元72可耦接處理單元71，儲存該第一索引模克樹及該第二索引模克樹。儲存單元72可為燒錄式光碟機、硬碟機、軟碟機、通用串行總線(USB)、動態隨機存取記憶體、快閃記憶體、電子抹除式可複寫唯讀記憶體(EEPROM)、可擦除可規劃式唯讀記憶體(EPROM)等，惟本發明不限於此。

【0063】另外，處理單元71比對該餘額資訊與該稽核資訊可比對該第一切片與該第二切片，該稽核資訊可至少對應一合約，且處理單元71處理該合約，儲存單元72儲存該合約。再者，該使用者與中介者可以該合約而交易，且該中介者令處理單元71更新該第一索引模克樹及該第二索引模克樹，於該使用者令處理單元71比對該餘額資訊與該稽核資訊異常時，處理單元71產生證據資訊予該合約，且儲存單元72儲存該證據資訊。而該中介者令處理單元71更新該第一索引模克樹及該第二索引模克樹可包含處理單元71產生對應該第一索引模克樹

之第一根雜湊值及對應該第二索引模克樹之第二根雜湊值，且該中介者令處理單元71以該第一根雜湊值及該第二根雜湊值更新該合約。

【0064】進一步而言，該使用者與該中介者之間具有溝通協定，且在該使用者之數目為複數個時，該些使用者之間具有證據協定，處理單元71處理該溝通協定及該證據協定，且儲存單元72儲存該溝通協定及該證據協定，在該交易之數目為複數個時，該中介者以一部分數目之該些交易作為一階段而令處理單元71更新該第一索引模克樹及該第二索引模克樹，儲存單元72儲存更新之該第一索引模克樹及該第二索引模克樹，且至少該第一索引模克樹與該第二索引模克樹之間具有各該階段完成時的清算協定，處理單元71處理該清算協定且儲存單元72儲存該清算協定。

【0065】如上所述之該合約可包含該中介者之抵押、該使用者之實體通貨兌換憑據或虛擬通貨、該使用者之實體通貨兌換憑據或虛擬通貨之儲金記錄、該合約與該第一索引模克樹及該第二索引模克樹之間的金流記錄、該些階段之序號、該第一索引模克樹及該第二索引模克樹之該些階段的雜湊值、以及該合約之函式。

【0066】如上所述之該合約之函式可包含將該使用者之實體通貨兌換憑據或該虛擬通貨存到該合約中的函式、將該使用者於該合約中的實體通貨兌換憑據或虛擬通貨轉移的函式、將該使用者於該合約中的實體通貨兌換憑據或虛擬通貨轉移至該第一索引模克樹的函式、將該第一索引模克樹之實體通貨兌換憑據或虛擬通貨的至少部分餘額轉移至該合約中的函式、結束一該階段並進行清算的函式、以及產生該證據資訊的函式。

【0067】如上所述之該溝通協定可包含轉帳交易、入金交易及出金交易。詳細而言，該轉帳交易之步驟可包含：該使用者令處理單元71送給該中介者T_{Rmit} = ((LSN, Remittance, Ui, Uj, X, 階段序號), $SIG_{Pri(Ui)}$)，LSN為該使用者產生的一

不重複的亂數，$SIG_{Pri(Ui)}$為該使用者所簽署之訊息本體的電子簽章；該中介者令處理單元71將該第一索引模克樹中的不同使用者(Ui,Uj)之該實體通貨兌換憑據或虛擬通貨的餘額修改，假定Ui及Uj之該實體通貨兌換憑據或虛擬通貨的餘額於轉帳後分別為p,q；該中介者令處理單元71以T_{ACK} = ((T_{Rmit}, p, q, GSN), $SIG_{Pri(Agent)}$)回覆該使用者Ui，GSN（Global sequence number）為該中介者產生的一個整數，由0開始，處理單元71每次處理一該使用者的交易後都會增加1予GSN，$SIG_{Pri(Agent)}$為該中介者所簽署之訊息本體的電子簽章；以及該中介者令處理單元71將T_{ACK}存到該第二索引模克樹。

【0068】 而該入金交易之步驟可包含：該使用者(Ui)令處理單元71送給該中介者$T_{Deposit}$ = ((LSN, Deposit, X, 階段序號), $SIG_{Pri(Ui)}$)， LSN為該使用者產生的一不重複的亂數，$SIG_{Pri(Ui)}$為該使用者所簽署之訊息本體的電子簽章；該中介者令處理單元71將該第一索引模克樹中的使用者餘額修改，假定該使用者之實體通貨兌換憑據或虛擬通貨的餘額於轉帳後為p；該中介者令處理單元71執行該合約中的Deposit_token_to_sidechain()，Deposit_token_to_sidechain()將該合約中的Ui.balance減去X，同時將該金流記錄增加一筆記錄：(Deposit, Ui, X, 階段序號, GSN)；該中介者令處理單元71以T_{ACK} = ((T_{Depost}, p, GSN), $SIG_{Pri(Agent)}$))回覆該使用者，GSN該中介者產生的一由0開始之整數，處理單元71每次處理一該使用者的交易後都會增加1予GSN，$SIG_{Pri(Agent)}$為該中介者所簽署之訊息本體的電子簽章；以及該中介者令處理單元71將T_{ACK}存到該第二索引模克樹。

【0069】 另外，該出金交易之步驟可包含：該使用者(Ui)令處理單元71送給該中介者$T_{Withdraw}$ = ((LSN, Withdraw, X, 階段序號), $SIG_{Pri(Ui)}$)，LSN為該使用者產生的一不重複的亂數，$SIG_{Pri(Ui)}$為該使用者所簽署之訊息本體的電子簽章；該中介者令處理單元71修改該第一索引模克樹中該使用者之餘額，假定該使用者之實體通貨兌換憑據或虛擬通貨的餘額於轉帳後為p；該中介者令處理單元71執

行該合約中的Withdraw_token_from_sidechain()，Withdraw_token_from_sidechain()將該合約中的Ui.balance加上X，同時將該金流記錄增加一筆記錄：(Withdraw, Ui, X, 階段序號, GSN)；該中介者令處理單元71以T_{ACK} = (($T_{Withdraw}$, p, GSN), $SIG_{Pri(Agent)}$) 回覆該使用者，GSN為該中介者產生的一由0開始之整數，處理單元71每次處理一該使用者的交易後都會增加1予GSN，$SIG_{Pri(Agent)}$為該中介者所簽署之訊息本體的電子簽章；以及該中介者令處理單元71將T_{ACK}存到該第二索引模克樹。

【0070】再者，該合約可更包含函式Finalize()，該中介者令處理單元71執行Finalize()以將該第一索引模克樹及該第二索引模克樹於現有階段結束後的雜湊值儲存於該合約並公布，同時該中介者公布該現有階段結束後的至少部分該第一索引模克樹及至少部分該第二索引模克樹以供查詢。

【0071】如上所述之該合約可具有函式Fraud_proof()以產生該證據資訊，該證據資訊可於以下情況或其組合產生：（1）該中介者於處理單元71處理轉帳交易、入金交易或出金交易後沒有將交易儲存於該第二索引模克樹，該使用者令處理單元71執行Fraud_proof()函式以提出由該中介者回傳的T_{ACK}及該第二索引模克樹的切片，證明該中介者沒有將該交易儲存於該第二索引模克樹；（2）該中介者於處理單元71處理該轉帳交易、該入金交易或該出金交易後將該使用者的餘額算錯，由於該中介者每個交易之回傳的T_{ACK}都有GSN，GSN之數值為遞增且不重複，故該使用者令處理單元71將該交易排序並找出發生錯誤交易的前一個交易的該中介者之回傳T_{ACK}，之後該使用者令處理單元71執行Fraud_proof()函式，將此錯誤交易及前一個交易的該中介者之回傳T_{ACK}為證據，而證明該中介者提不出有GSN值介於此兩交易中GSN值的交易以證明該中介者出錯。

【0072】此外，該第一索引模克樹及該第二索引模克樹可對應一區塊鏈。實際而言，該區塊鏈可外接於本發明之分散式金流稽核裝置7或為分散式金流稽核裝置7內含之區塊鏈單元73，而區塊鏈單元73可至少與處理單元71耦接。。

【0073】須注意的是，本發明之一種分散式金流稽核裝置7的其它內容已於上文敘述，不再贅述。另外，該使用者或該中介者令處理單元71執行之指令可由該使用者或該中介者直接輸入分散式金流稽核裝置7，或可由該使用者或該中介者從外接裝置輸入分散式金流稽核裝置7。再者，該耦接可為電性耦接及/或光學耦接等可傳遞訊號或指令的耦接方式。

【0074】如圖8所示，其係本發明之一種分散式金流稽核系統8的方塊圖，其可包括複數個金流稽核裝置81。如上所述之複數個金流稽核裝置81的其中至少一者可包含處理單元811或儲存單元812，且該些金流稽核裝置81具有資料傳輸單元813，處理單元811產生相關於使用者且為實體通貨兌換憑據或虛擬通貨之餘額資訊的第一索引模克樹、產生相關於該餘額資訊之交易的稽核資訊之第二索引模克樹、比對該餘額資訊與該稽核資訊或其組合，資料傳輸單元813可傳輸至少部分對應該第一索引模克樹之資訊、至少部分對應該第二索引模克樹之資訊、該餘額資訊與該稽核資訊之比對結果或其組合，儲存單元812耦接處理單元811或資料傳輸單元813，以儲存該第一索引模克樹或該第二索引模克樹。即在分散式計算架構或雲計算的情況下，金流稽核裝置81可不必同時具有處理單元811或儲存單元812，或不必同時具有上述分散式金流稽核系統8之功能的處理單元811或儲存單元812，惟金流稽核裝置81可具有資料傳輸單元813以供分散式金流稽核系統8之運作。而第一索引模克樹、第二索引模克樹、該餘額資訊與該稽核資訊之比對或其組合可在不同處理單元811中進行，且該第一索引模克樹及該第二索引模克樹可在不同儲存單元812中儲存。

【0075】另外，該第一索引模克樹可包含第一切片且該第二索引模克樹可包含第二切片，進一步而言，處理單元811比對該餘額資訊與該稽核資訊可比對該第一切片與該第二切片。而該稽核資訊可至少對應一合約，且至少一該處理單元811處理該合約，至少一儲存單元812儲存該合約。

【0076】在本發明之另一態樣中，使用者與中介者可以該合約而交易，且該中介者於交易後令至少一處理單元811更新該第一索引模克樹及該第二索引模克樹，於該使用者令至少一處理單元811比對該餘額資訊與該稽核資訊異常時，至少一處理單元811產生證據資訊予該合約，且至少一儲存單元812儲存該證據資訊。

【0077】實際而言，該使用者與該中介者之間具有溝通協定，且在該使用者之數目為複數個時，該些使用者之間具有證據協定，至少一處理單元811處理該溝通協定及該證據協定，且至少一儲存單元812儲存該溝通協定及該證據協定，在該交易之數目為複數個時，該中介者以一部分數目之該些交易作為一階段而令至少一處理單元811更新該第一索引模克樹及該第二索引模克樹，至少一儲存單元812儲存更新之該第一索引模克樹及該第二索引模克樹，且至少該第一索引模克樹與該第二索引模克樹之間具有各該階段完成時的清算協定，至少一處理單元811處理該清算協定且至少一儲存單元812儲存該清算協定。而該溝通協定可包含轉帳交易、入金交易及出金交易。

【0078】另外，該合約可包含該中介者之抵押、該使用者之實體通貨兌換憑據或虛擬通貨、該使用者之實體通貨兌換憑據或虛擬通貨之儲金記錄、該合約與該第一索引模克樹及該第二索引模克樹之間的金流記錄、該些階段之序號、該第一索引模克樹及該第二索引模克樹之該些階段的雜湊值、以及該合約之函式。

【0079】如上所述之該轉帳交易之步驟可包含：該使用者令至少一處理單元811送給該中介者T_{Rmit} = ((LSN, Remittance, Ui, Uj, X, 階段序號), $SIG_{Pri(Ui)}$)，LSN為該使用者產生的一不重複的亂數，$SIG_{Pri(Ui)}$為該使用者所簽署之訊息本體的電子簽章；該中介者令至少一處理單元811將該第一索引模克樹中的不同使用者(Ui,Uj)之該實體通貨兌換憑據或虛擬通貨的餘額修改，假定Ui及Uj之該實體通貨兌換憑據或虛擬通貨的餘額於轉帳後分別為p,q；該中介者令至少一處理單元811以T_{ACK} = ((T_{Rmit}, p, q, GSN), $SIG_{Pri(Agent)}$)回覆該使用者Ui，GSN為該中介者產生的一個整數，由0開始，至少一處理單元811每次處理一該使用者的交易後都會增加1予GSN，$SIG_{Pri(Agent)}$為該中介者所簽署之訊息本體的電子簽章；以及該中介者令至少一處理單元811將T_{ACK}存到該第二索引模克樹。

【0080】如上所述之該入金交易之步驟可包含：該使用者(Ui)令至少一處理單元811送給該中介者$T_{Deposit}$ = ((LSN, Deposit, X, 階段序號), $SIG_{Pri(Ui)}$)， LSN為該使用者產生的一不重複的亂數，$SIG_{Pri(Ui)}$為該使用者所簽署之訊息本體的電子簽章；該中介者令至少一處理單元811將該第一索引模克樹中的使用者餘額修改，假定該使用者之實體通貨兌換憑據或虛擬通貨的餘額於轉帳後為p；該中介者令至少一處理單元811執行該合約中的Deposit_token_to_sidechain()，Deposit_token_to_sidechain()將該合約中的Ui.balance減去X，同時將該金流記錄增加一筆記錄：(Deposit, Ui, X, 階段序號, GSN)；該中介者令至少一處理單元811以T_{ACK} = ((T_{Depost}, p, GSN), $SIG_{Pri(Agent)}$))回覆該使用者，GSN為該中介者產生的一由0開始之整數，至少一處理單元811每次處理一該使用者的交易後都會增加1予GSN，$SIG_{Pri(Agent)}$為該中介者所簽署之訊息本體的電子簽章；以及該中介者令至少一處理單元811將T_{ACK}存到該第二索引模克樹。

【0081】如上所述之該出金交易之步驟可包含：該使用者(Ui)令至少一處理單元811送給該中介者$T_{Withdraw}$ = ((LSN, Withdraw, X, 階段序號), $SIG_{Pri(Ui)}$)，LSN

為該使用者產生的一不重複的亂數，$SIG_{Pri(Ui)}$為該使用者所簽署之訊息本體的電子簽章；該中介者令至少一處理單元811修改該第一索引模克樹中該使用者之餘額，假定該使用者之實體通貨兌換憑據或虛擬通貨的餘額於轉帳後為p；該中介者令至少一處理單元811執行該合約中的Withdraw_token_from_sidechain()，Withdraw_token_from_sidechain()將該合約中的Ui.balance加上X，同時將該金流記錄增加一筆記錄：(Withdraw, Ui, X, 階段序號, GSN)；該中介者令至少一處理單元811以T_{ACK} = (($T_{Withdraw}$, p, GSN), $SIG_{Pri(Agent)}$) 回覆該使用者，GSN為該中介者產生的一由0開始之整數，至少一處理單元811每次處理一該使用者的交易後都會增加1予GSN，$SIG_{Pri(Agent)}$為該中介者所簽署之訊息本體的電子簽章；以及該中介者令至少一處理單元811將T_{ACK}存到該第二索引模克樹。

【0082】另外，該合約具有函式Finalize()，該中介者令至少一處理單元811執行Finalize()以將該第一索引模克樹及該第二索引模克樹於現有階段結束後的雜湊值儲存於該合約並公布，同時該中介者公布該現有階段結束後的至少部分該第一索引模克樹及至少部分該第二索引模克樹以供查詢。

【0083】再者，該合約可具有函式Fraud_proof()以產生該證據資訊，該證據資訊可於以下情況或其組合產生：（1）該中介者於至少一處理單元811處理轉帳交易、入金交易或出金交易後沒有將交易儲存於該第二索引模克樹，該使用者令至少一處理單元811執行Fraud_proof()函式以提出由該中介者回傳的T_{ACK}及該第二索引模克樹的切片，證明該中介者沒有將該交易儲存於該第二索引模克樹；（2）該中介者於至少一處理單元811處理該轉帳交易、該入金交易或該出金交易後將該使用者的餘額算錯，由於該中介者每個交易之回傳的T_{ACK}都有GSN，GSN之數值為遞增且不重複，故該使用者令至少一處理單元811將該交易排序並找出發生錯誤交易的前一個交易的該中介者之回傳T_{ACK}，之後該使用者令至少一處理單元811執行Fraud_proof()函式，將此錯誤交易及前一個交

易的該中介者之回傳T_{ACK}為證據，而證明該中介者提不出有GSN值介於此兩交易中GSN值的交易以證明該中介者出錯。

【0084】進一步而言，該中介者令至少一處理單元811更新該第一索引模克樹及該第二索引模克樹可包含至少一處理單元811產生對應該第一索引模克樹之第一根雜湊值且至少一處理單元811產生對應該第二索引模克樹之第二根雜湊值，且該中介者令至少一處理單元811以該第一根雜湊值及該第二根雜湊值更新該合約，資料傳輸單元813傳輸該第一根雜湊值及該第二根雜湊值。

【0085】在本發明之另一態樣中，本發明之一種分散式金流稽核系統8可更包括區塊鏈裝置82或區塊鏈單元814，區塊鏈裝置82與至少一金流稽核裝置81耦接，區塊鏈單元814設置於至少一金流稽核裝置81，該第一索引模克樹及該第二索引模克樹可至少對應區塊鏈裝置82或區塊鏈單元814中之一區塊鏈。

【0086】綜上所述，本發明藉由將複數筆交易之累積稽核資訊整合為單一稽核資訊，可從而節省傳輸稽核資訊之時間、次數、手續費等成本。另外，藉由中介者提供一筆抵押以於該使用者比對該餘額資訊與該稽核資訊異常時由該抵押支付賠償予該使用者，從而提升本發明之公信力。再者，本發明藉由使用者僅比對原始帳本(稽核資訊)之切片，從而達成低負擔且高效率之系統。此外，本發明還藉由各種協定而建立複數個使用者之間及使用者與至少一個中介者之間的多對多交易管道以支援實體通貨兌換憑據或虛擬通貨的一般性微支付。

【0087】本發明在上文中已以較佳實施例揭露，然熟習本項技術者應理解的是，該實施例僅用於描繪本發明，而不應解讀為限制本發明之範圍。應注意的是，舉凡與該實施例等效之變化與置換，均應設為涵蓋於本發明之範疇內。因此，本發明之保護範圍當以申請專利範圍所界定者為準。

【符號說明】

【0088】

7	分散式金流稽核裝置
71、811	處理單元
72、812	儲存單元
8	分散式金流稽核系統
81	金流稽核裝置
813	資料傳輸單元
73、814	區塊鏈單元
82	區塊鏈裝置
S10、S11、S401、S402、S403、S404、S501、S502、S503、S504、S505、S601、S602、S603、S604、S605	步驟

202004626
專利案號：107117106
申請日：
IPC 分類：
202004626

【發明摘要】

【中文發明名稱】　分散式金流稽核方法、裝置及系統

【中文】

本發明係一種分散式金流稽核方法、裝置及系統，該分散式金流稽核方法包括提供相關於使用者且儲存為第一索引模克樹的實體通貨兌換憑據或虛擬通貨之餘額資訊及相關於該餘額資訊且儲存為第二索引模克樹之交易的稽核資訊；以及該使用者比對該餘額資訊與該稽核資訊。該分散式金流稽核方法更包括該使用者與該中介者之間的溝通協定、該些使用者之間的證據協定及該第一索引模克樹與該第二索引模克樹之間所具有各階段完成時的清算協定。本發明能解決現有區塊鏈交易成本過高、公信力不佳及低效率等問題，並能支援實體通貨兌換憑據或虛擬通貨的一般性微支付。

【指定代表圖】　圖 1

【代表圖之符號簡單說明】

S10、S11　步驟

【發明申請專利範圍】

【第1項】一種分散式金流稽核方法，係包括：

提供相關於使用者且儲存為第一索引模克樹的實體通貨兌換憑據或虛擬通貨之餘額資訊及相關於該餘額資訊且儲存為第二索引模克樹之交易的稽核資訊；以及

該使用者比對該餘額資訊與該稽核資訊。

【第2項】如申請專利範圍第1項所述之分散式金流稽核方法，其中，該稽核資訊係至少對應一合約。

【第3項】如申請專利範圍第2項所述之分散式金流稽核方法，其中，該使用者係與中介者以該合約而交易，且該中介者於該交易後更新該第一索引模克樹及該第二索引模克樹，於該使用者比對該餘額資訊與該稽核資訊異常時，產生證據資訊予該合約。

【第4項】如申請專利範圍第3項所述之分散式金流稽核方法，其中，該使用者與該中介者之間具有溝通協定，且在該使用者之數目為複數個時，該些使用者之間具有證據協定，在該交易之數目為複數個時，該中介者以一部分數目之該些交易作為一階段而更新該第一索引模克樹及該第二索引模克樹，且至少該第一索引模克樹與該第二索引模克樹之間具有各該階段完成時的清算協定。

【第5項】如申請專利範圍第4項所述之分散式金流稽核方法，其中，該合約包含該中介者之抵押、該使用者之實體通貨兌換憑據或虛擬通貨、該使用者之實體通貨兌換憑據或虛擬通貨之儲金記錄、該合約與該第一索引模克樹及該第二索引模克樹之間的金流記錄、該

些階段之序號、該第一索引模克樹及該第二索引模克樹之該些階段的雜湊值、以及該合約之函式。

【第6項】如申請專利範圍第5項所述之分散式金流稽核方法，其中，該合約之函式包含將該使用者之實體通貨兌換憑據或該虛擬通貨存到該合約中的函式、將該使用者於該合約中的實體通貨兌換憑據或虛擬通貨轉移的函式、將該使用者於該合約中的實體通貨兌換憑據或虛擬通貨轉移至該第一索引模克樹的函式、將該第一索引模克樹之實體通貨兌換憑據或虛擬通貨的至少部分餘額轉移至該合約中的函式、結束一該階段並進行清算的函式、以及產生該證據資訊的函式。

【第7項】如申請專利範圍第4項所述之分散式金流稽核方法，其中，該溝通協定包含轉帳交易、入金交易及出金交易。

【第8項】如申請專利範圍第7項所述之分散式金流稽核方法，其中，該轉帳交易之步驟包含：該使用者送給該中介者T_{Rmit} = ((LSN, Remittance, Ui, Uj, X, 階段序號), $SIG_{Pri(Ui)}$)，LSN為該使用者產生的一不重複的亂數，$SIG_{Pri(Ui)}$為該使用者所簽署之訊息本體的電子簽章；該中介者將該第一索引模克樹中的不同使用者(Ui,Uj)之該實體通貨兌換憑據或虛擬通貨的餘額修改，假定Ui及Uj之該實體通貨兌換憑據或虛擬通貨的餘額於轉帳後分別為p,q；該中介者以T_{ACK} = ((T_{Rmit}, p, q, GSN), $SIG_{Pri(Agent)}$)回覆該使用者Ui， GSN為該中介者產生的一個整數，由0開始，每次處理一該使用者的交易後都會增加1予GSN，$SIG_{Pri(Agent)}$為該中介者所簽署之訊息本體的電子簽章；以及該中介者將T_{ACK}存到該第二索引模克樹。

【第9項】如申請專利範圍第7項所述之分散式金流稽核方法，其中，該入金交易之步驟包含：該使用者(Ui)送給該中介者$T_{Deposit}$ = ((LSN, Deposit, X, 階段序號), $SIG_{Pri(Ui)}$)， LSN為該使用者產生的一不重複的亂數，$SIG_{Pri(Ui)}$為該使用者所簽署之訊息本體的電子簽章；該中介者將該第一索引模克樹中的使用者餘額修改，假定該使用者之實體通貨兌換憑據或虛擬通貨的餘額於轉帳後為p；該中介者令該合約中的Deposit_token_to_sidechain()執行，Deposit_token_to_sidechain()將該合約中的Ui.balance減去X，同時將該金流記錄增加一筆記錄：(Deposit, Ui, X, 階段序號, GSN)；該中介者以T_{ACK} = ((T_{Depost}, p, GSN), $SIG_{Pri(Agent)}$))回覆該使用者，GSN為該中介者產生的一由0開始之整數，每次處理一該使用者的交易後都會增加1予GSN，$SIG_{Pri(Agent)}$為該中介者所簽署之訊息本體的電子簽章；以及該中介者將T_{ACK}存到該第二索引模克樹。

【第10項】如申請專利範圍第7項所述之分散式金流稽核方法，其中，該出金交易之步驟包含：該使用者(Ui)送給該中介者$T_{Withdraw}$ = ((LSN, Withdraw, X, 階段序號), $SIG_{Pri(Ui)}$)，LSN為該使用者產生的一不重複的亂數，$SIG_{Pri(Ui)}$為該使用者所簽署之訊息本體的電子簽章；該中介者修改該第一索引模克樹中該使用者之餘額，假定該使用者之實體通貨兌換憑據或虛擬通貨的餘額於轉帳後為p；該中介者令該合約中的Withdraw_token_from_sidechain()執行，Withdraw_token_from_sidechain()將該合約中的Ui.balance加上X，同時將該金流記錄增加一筆記錄：(Withdraw, Ui, X, 階段序號, GSN)；該中介者以T_{ACK} = (($T_{Withdraw}$, p, GSN), $SIG_{Pri(Agent)}$) 回覆該

使用者，GSN為該中介者產生的一由0開始之整數，每次處理一該使用者的交易後都會增加1予GSN，$SIG_{Pri(Agent)}$為該中介者所簽署之訊息本體的電子簽章；以及該中介者將T_{ACK}存到該第二索引模克樹。

【第11項】如申請專利範圍第5項所述之分散式金流稽核方法，其中，該合約更包含函式Finalize()，該中介者執行Finalize()以將該第一索引模克樹及該第二索引模克樹於現有階段結束後的雜湊值儲存於該合約並公布，同時該中介者公布該現有階段結束後的至少部分該第一索引模克樹及至少部分該第二索引模克樹以供查詢。

【第12項】如申請專利範圍第6項所述之分散式金流稽核方法，其中，該合約具有函式Fraud_proof()以產生該證據資訊，該證據資訊係於以下情況或其組合產生：（1）該中介者於處理轉帳交易、入金交易或出金交易後沒有將交易儲存於該第二索引模克樹，該使用者執行Fraud_proof()函式以提出由該中介者回傳的T_{ACK}及該第二索引模克樹的切片，證明該中介者沒有將該交易儲存於該第二索引模克樹；（2）該中介者於處理該轉帳交易、該入金交易或該出金交易後將該使用者的餘額算錯，由於該中介者每個交易之回傳的T_{ACK}都有GSN，其數值為遞增且不重複，故該使用者將該交易排序並找出發生錯誤交易的前一個交易的該中介者之回傳T_{ACK}，之後該使用者執行Fraud_proof()函式，將此錯誤交易及前一個交易的該中介者之回傳T_{ACK}為證據，而證明該中介者提不出有GSN值介於此兩交易中GSN值的交易以證明該中介者出錯。

【第13項】如申請專利範圍第1項所述之分散式金流稽核方法，其中，該第一索引模克樹及該第二索引模克樹係對應一區塊鏈。

【第14項】一種分散式金流稽核裝置，係包括：

處理單元，產生相關於使用者且為實體通貨兌換憑據或虛擬通貨之餘額資訊的第一索引模克樹，以及產生相關於該餘額資訊之交易的稽核資訊之第二索引模克樹，且比對該餘額資訊與該稽核資訊；以及

儲存單元，耦接該處理單元，儲存該第一索引模克樹及該第二索引模克樹。

【第15項】如申請專利範圍第14項所述之分散式金流稽核裝置，其中，該稽核資訊係至少對應一合約，且該處理單元處理該合約，該儲存單元儲存該合約。

【第16項】如申請專利範圍第15項所述之分散式金流稽核裝置，其中，該使用者與中介者係以該合約而交易，且該中介者於交易後令該處理單元更新該第一索引模克樹及該第二索引模克樹，於該使用者令該處理單元比對該餘額資訊與該稽核資訊異常時，該處理單元產生證據資訊予該合約，該儲存單元儲存該證據資訊。

【第17項】如申請專利範圍第16項所述之分散式金流稽核裝置，其中，該使用者與該中介者之間具有溝通協定，且在該使用者之數目為複數個時，該些使用者之間具有證據協定，該處理單元處理該溝通協定及該證據協定，且該儲存單元儲存該溝通協定及該證據協定，在該交易之數目為複數個時，該中介者以一部分數目之該些交易作為一階段而令該處理單元更新該第一索引模克樹及該第二索引模克樹，該儲存單元儲存更新之該第一索引模克樹及該第二索引模克樹，且至少該第一索引模克樹與該第二索引模克樹之間

具有各該階段完成時的清算協定，該處理單元處理該清算協定且該儲存單元儲存該清算協定。

【第18項】如申請專利範圍第17項所述之分散式金流稽核裝置，其中，該合約包含該中介者之抵押、該使用者之實體通貨兌換憑據或虛擬通貨、該使用者之實體通貨兌換憑據或虛擬通貨之儲金記錄、該合約與該第一索引模克樹及該第二索引模克樹之間的金流記錄、該些階段之序號、該第一索引模克樹及該第二索引模克樹之該些階段的雜湊值、以及該合約之函式。

【第19項】如申請專利範圍第18項所述之分散式金流稽核裝置，其中，該合約之函式包含將該使用者之實體通貨兌換憑據或該虛擬通貨存到該合約中的函式、將該使用者於該合約中的實體通貨兌換憑據或虛擬通貨轉移的函式、將該使用者於該合約中的實體通貨兌換憑據或虛擬通貨轉移至該第一索引模克樹的函式、將該第一索引模克樹之實體通貨兌換憑據或虛擬通貨的至少部分餘額轉移至該合約中的函式、結束一該階段並進行清算的函式、以及產生該證據資訊的函式。

【第20項】如申請專利範圍第17項所述之分散式金流稽核裝置，其中，該溝通協定包含轉帳交易、入金交易及出金交易。

【第21項】如申請專利範圍第20項所述之分散式金流稽核裝置，其中，該轉帳交易之步驟包含：該使用者令該處理單元送給該中介者T_{Rmit} = ((LSN, Remittance, Ui, Uj, X, 階段序號), $SIG_{Pri(Ui)}$)，LSN為該使用者產生的一不重複的亂數，$SIG_{Pri(Ui)}$為該使用者所簽署之訊息本體的電子簽章；該中介者令該處理單元將該第一索引模克樹中的不同使用者(Ui,Uj)之該實體通貨兌換憑據或虛擬通貨的餘額修改，假

定Ui及Uj之該實體通貨兌換憑據或虛擬通貨的餘額於轉帳後分別為p,q；該中介者令該處理單元以T_{ACK} = ((T_{Rmit}, p, q, GSN), $SIG_{Pri(Agent)}$)回覆該使用者Ui，GSN為該中介者產生的一個整數，由0開始，該處理單元每次處理一該使用者的交易後都會增加1予GSN，$SIG_{Pri(Agent)}$為該中介者所簽署之訊息本體的電子簽章；以及該中介者令該處理單元將T_{ACK}存到該第二索引模克樹。

【第22項】如申請專利範圍第20項所述之分散式金流稽核裝置，其中，該入金交易之步驟包含：該使用者(Ui)令該處理單元送給該中介者$T_{Deposit}$ = ((LSN, Deposit, X, 階段序號), $SIG_{Pri(Ui)}$)， LSN為該使用者產生的一不重複的亂數，$SIG_{Pri(Ui)}$為該使用者所簽署之訊息本體的電子簽章；該中介者令該處理單元將該第一索引模克樹中的使用者餘額修改，假定該使用者之實體通貨兌換憑據或虛擬通貨的餘額於轉帳後為p；該中介者令該處理單元執行該合約中的Deposit_token_to_sidechain()，Deposit_token_to_sidechain()將該合約中的Ui.balance減去X，同時將該金流記錄增加一筆記錄：(Deposit, Ui, X, 階段序號, GSN)；該中介者令該處理單元以T_{ACK} = ((T_{Depost}, p, GSN), $SIG_{Pri(Agent)}$))回覆該使用者，GSN為該中介者產生的一由0開始之整數，該處理單元每次處理一該使用者的交易後都會增加1予GSN，$SIG_{Pri(Agent)}$為該中介者所簽署之訊息本體的電子簽章；以及該中介者令該處理單元將T_{ACK}存到該第二索引模克樹。

【第23項】如申請專利範圍第20項所述之分散式金流稽核裝置，其中，該出金交易之步驟包含：該使用者(Ui)令該處理單元送給該中介者$T_{Withdraw}$ = ((LSN, Withdraw, X, 階段序號), $SIG_{Pri(Ui)}$)，LSN為該使

用者產生的一不重複的亂數，$SIG_{Pri(Ui)}$為該使用者所簽署之訊息本體的電子簽章；該中介者令該處理單元修改該第一索引模克樹中該使用者之餘額，假定該使用者之實體通貨兌換憑據或虛擬通貨的餘額於轉帳後為p；該中介者令該處理單元執行該合約中的Withdraw_token_from_sidechain()，Withdraw_token_from_sidechain()將該合約中的Ui.balance加上X，同時將該金流記錄增加一筆記錄：(Withdraw, Ui, X, 階段序號, GSN)；該中介者令該處理單元以T_{ACK} = (($T_{Withdraw}$, p, GSN), $SIG_{Pri(Agent)}$) 回覆該使用者，GSN為該中介者產生的一由0開始之整數，該處理單元每次處理一該使用者的交易後都會增加1予GSN，$SIG_{Pri(Agent)}$為該中介者所簽署之訊息本體的電子簽章；以及該中介者令該處理單元將T_{ACK}存到該第二索引模克樹。

【第24項】如申請專利範圍第18項所述之分散式金流稽核裝置，其中，該合約更包含函式Finalize()，該中介者令該處理單元執行Finalize()以將該第一索引模克樹及該第二索引模克樹於現有階段結束後的雜湊值儲存於該合約並公布，同時該中介者公布該現有階段結束後的至少部分該第一索引模克樹及至少部分該第二索引模克樹以供查詢。

【第25項】如申請專利範圍第19項所述之分散式金流稽核裝置，其中，該合約具有函式Fraud_proof()以產生該證據資訊，該證據資訊係於以下情況或其組合產生：（1）該中介者於該處理單元處理轉帳交易、入金交易或出金交易後沒有將交易儲存於該第二索引模克樹，該使用者令該處理單元執行Fraud_proof()函式以提出由該中介者回傳的T_{ACK}及該第二索引模克樹的切片，證明該中介者沒有

將該交易儲存於該第二索引模克樹；（2）該中介者於該處理單元處理該轉帳交易、該入金交易或該出金交易後將該使用者的餘額算錯，由於該中介者每個交易之回傳的T_{ACK}都有GSN，GSN之數值為遞增且不重複，故該使用者令該處理單元將該交易排序並找出發生錯誤交易的前一個交易的該中介者之回傳T_{ACK}，之後該使用者令該處理單元執行Fraud_proof()函式，將此錯誤交易及前一個交易的該中介者之回傳T_{ACK}為證據，而證明該中介者提不出有GSN值介於此兩交易中GSN值的交易以證明該中介者出錯。

【第26項】如申請專利範圍第14項所述之分散式金流稽核裝置，其中，該第一索引模克樹及該第二索引模克樹係對應一區塊鏈。

【第27項】一種分散式金流稽核系統，係包括：

複數個金流稽核裝置，其至少一者係包含處理單元或儲存單元，且該些金流稽核裝置具有資料傳輸單元，至少一該處理單元產生相關於使用者且為實體通貨兌換憑據或虛擬通貨之餘額資訊的第一索引模克樹、產生相關於該餘額資訊之交易的稽核資訊之第二索引模克樹、比對該餘額資訊與該稽核資訊或其組合，該資料傳輸單元傳輸至少部分對應該第一索引模克樹之資訊、至少部分對應該第二索引模克樹之資訊、該餘額資訊與該稽核資訊之比對結果或其組合，該儲存單元耦接該處理單元或該資料傳輸單元，以儲存該第一索引模克樹或該第二索引模克樹。

【第28項】如申請專利範圍第27項所述之分散式金流稽核系統，其中，該稽核資訊係至少對應一合約，且至少一該處理單元處理該合約，至少一該儲存單元儲存該合約。

【第29項】如申請專利範圍第28項所述之分散式金流稽核系統，其中，該使用者係與中介者以該合約而交易，且該中介者於交易後令至少一該處理單元更新該第一索引模克樹及該第二索引模克樹，於該使用者令至少一該處理單元比對該餘額資訊與該稽核資訊異常時，至少一該處理單元產生證據資訊予該合約，且至少一該儲存單元儲存該證據資訊。

【第30項】如申請專利範圍第29項所述之分散式金流稽核系統，其中，該使用者與該中介者之間具有溝通協定，且在該使用者之數目為複數個時，該些使用者之間具有證據協定，至少一該處理單元處理該溝通協定及該證據協定，且至少一該儲存單元儲存該溝通協定及該證據協定，在該交易之數目為複數個時，該中介者以一部分數目之該些交易作為一階段而令至少一該處理單元更新該第一索引模克樹及該第二索引模克樹，至少一該儲存單元儲存更新之該第一索引模克樹及該第二索引模克樹，且至少該第一索引模克樹與該第二索引模克樹之間具有各該階段完成時的清算協定，至少一該處理單元處理該清算協定且至少一該儲存單元儲存該清算協定。

【第31項】如申請專利範圍第30項所述之分散式金流稽核系統，其中，該合約包含該中介者之抵押、該使用者之實體通貨兌換憑據或虛擬通貨、該使用者之實體通貨兌換憑據或虛擬通貨之儲金記錄、該合約與該第一索引模克樹及該第二索引模克樹之間的金流記錄、該些階段之序號、該第一索引模克樹及該第二索引模克樹之該些階段的雜湊值、以及該合約之函式。

【第32項】如申請專利範圍第31項所述之分散式金流稽核系統，其中，該合約之函式包含將該使用者之實體通貨兌換憑據或該虛擬通貨存到該合約中的函式、將該使用者於該合約中的實體通貨兌換憑據或虛擬通貨轉移的函式、將該使用者於該合約中的實體通貨兌換憑據或虛擬通貨轉移至該第一索引模克樹的函式、將該第一索引模克樹之實體通貨兌換憑據或虛擬通貨的至少部分餘額轉移至該合約中的函式、結束一該階段並進行清算的函式、以及產生該證據資訊的函式。

【第33項】如申請專利範圍第30項所述之分散式金流稽核系統，其中，該溝通協定包含轉帳交易、入金交易及出金交易。

【第34項】如申請專利範圍第33項所述之分散式金流稽核系統，其中，該轉帳交易之步驟包含：該使用者令至少一該處理單元送給該中介者T_{Rmit} = ((LSN, Remittance, Ui, Uj, X, 階段序號), $SIG_{Pri(Ui)}$)，LSN為該使用者產生的一不重複的亂數，$SIG_{Pri(Ui)}$為該使用者所簽署之訊息本體的電子簽章；該中介者令至少一該處理單元將該第一索引模克樹中的不同使用者(Ui,Uj)之該實體通貨兌換憑據或虛擬通貨的餘額修改，假定Ui及Uj之該實體通貨兌換憑據或虛擬通貨的餘額於轉帳後分別為p,q；該中介者令至少一該處理單元以T_{ACK} = ((T_{Rmit}, p, q, GSN), $SIG_{Pri(Agent)}$)回覆該使用者Ui，GSN為該中介者產生的一個整數，由0開始，至少一該處理單元每次處理一該使用者的交易後都會增加1予GSN，$SIG_{Pri(Agent)}$為該中介者所簽署之訊息本體的電子簽章；以及該中介者令至少一該處理單元將T_{ACK}存到該第二索引模克樹。

【第35項】如申請專利範圍第33項所述之分散式金流稽核系統，其中，該入金交易之步驟包含：該使用者(Ui)令至少一該處理單元送給該中介者$T_{Deposit}$ = ((LSN, Deposit, X, 階段序號), $SIG_{Pri(Ui)}$)， LSN為該使用者產生的一不重複的亂數，$SIG_{Pri(Ui)}$為該使用者所簽署之訊息本體的電子簽章；該中介者令至少一該處理單元將該第一索引模克樹中的使用者餘額修改，假定該使用者之實體通貨兌換憑據或虛擬通貨的餘額於轉帳後為p；該中介者令至少一該處理單元執行該合約中的Deposit_token_to_sidechain()，Deposit_token_to_sidechain()將該合約中的Ui.balance減去X，同時將該金流記錄增加一筆記錄：(Deposit, Ui, X, 階段序號, GSN)；該中介者令至少一該處理單元以T_{ACK} = ((T_{Depost}, p, GSN), $SIG_{Pri(Agent)}$))回覆該使用者，GSN為該中介者產生的一由0開始之整數，至少一該處理單元每次處理一該使用者的交易後都會增加1予GSN，$SIG_{Pri(Agent)}$為該中介者所簽署之訊息本體的電子簽章；以及該中介者令至少一該處理單元將T_{ACK}存到該第二索引模克樹。

【第36項】如申請專利範圍第33項所述之分散式金流稽核系統，其中，該出金交易之步驟包含：該使用者(Ui)令至少一該處理單元送給該中介者$T_{Withdraw}$ = ((LSN, Withdraw, X, 階段序號), $SIG_{Pri(Ui)}$)，LSN為該使用者產生的一不重複的亂數，$SIG_{Pri(Ui)}$為該使用者所簽署之訊息本體的電子簽章；該中介者令至少一該處理單元修改該第一索引模克樹中該使用者之餘額，假定該使用者之實體通貨兌換憑據或虛擬通貨的餘額於轉帳後為p；該中介者令至少一該處理單元執行該合約中的Withdraw_token_from_sidechain()，Withdraw_token_from_sidechain()將該合約中的Ui.balance加上

X，同時將該金流記錄增加一筆記錄：(Withdraw, Ui, X, 階段序號, GSN)；該中介者令至少一該處理單元以T_{ACK} = (($T_{Withdraw}$, p, GSN), $SIG_{Pri(Agent)}$) 回覆該使用者，GSN為該中介者產生的一由0開始之整數，至少一該處理單元每次處理一該使用者的交易後都會增加1予GSN，$SIG_{Pri(Agent)}$為該中介者所簽署之訊息本體的電子簽章；以及該中介者令至少一該處理單元將T_{ACK}存到該第二索引模克樹。

【第37項】如申請專利範圍第31項所述之分散式金流稽核系統，其中，該合約更包含函式Finalize()，該中介者令至少一該處理單元執行Finalize()以將該第一索引模克樹及該第二索引模克樹於現有階段結束後的雜湊值儲存於該合約並公布，同時該中介者公布該現有階段結束後的至少部分該第一索引模克樹及至少部分該第二索引模克樹以供查詢。

【第38項】如申請專利範圍第32項所述之分散式金流稽核系統，其中，該合約具有函式Fraud_proof()以產生該證據資訊，該證據資訊係於以下情況或其組合產生：（1）該中介者於至少一該處理單元處理轉帳交易、入金交易或出金交易後沒有將交易儲存於該第二索引模克樹，該使用者令至少一該處理單元執行Fraud_proof()函式以提出由該中介者回傳的T_{ACK}及該第二索引模克樹的切片，證明該中介者沒有將該交易儲存於該第二索引模克樹；（2）該中介者於至少一該處理單元處理該轉帳交易、該入金交易或該出金交易後將該使用者的餘額算錯，由於該中介者每個交易之回傳的T_{ACK}都有GSN，GSN之數值為遞增且不重複，故該使用者令至少一該處理單元將該交易排序並找出發生錯誤交易的前一個交易的該中介

者之回傳T_{ACK}，之後該使用者令至少一該處理單元執行Fraud_proof()函式，將此錯誤交易及前一個交易的該中介者之回傳T_{ACK}為證據，而證明該中介者提不出有GSN值介於此兩交易中GSN值的交易以證明該中介者出錯。

【第39項】如申請專利範圍第27項所述之分散式金流稽核系統，更包括區塊鏈裝置或區塊鏈單元，該區塊鏈裝置與至少一該金流稽核裝置耦接，該區塊鏈單元設置於至少一該金流稽核裝置，該第一索引模克樹及該第二索引模克樹係至少對應該區塊鏈裝置或該區塊鏈單元中之一區塊鏈。

【發明圖式】

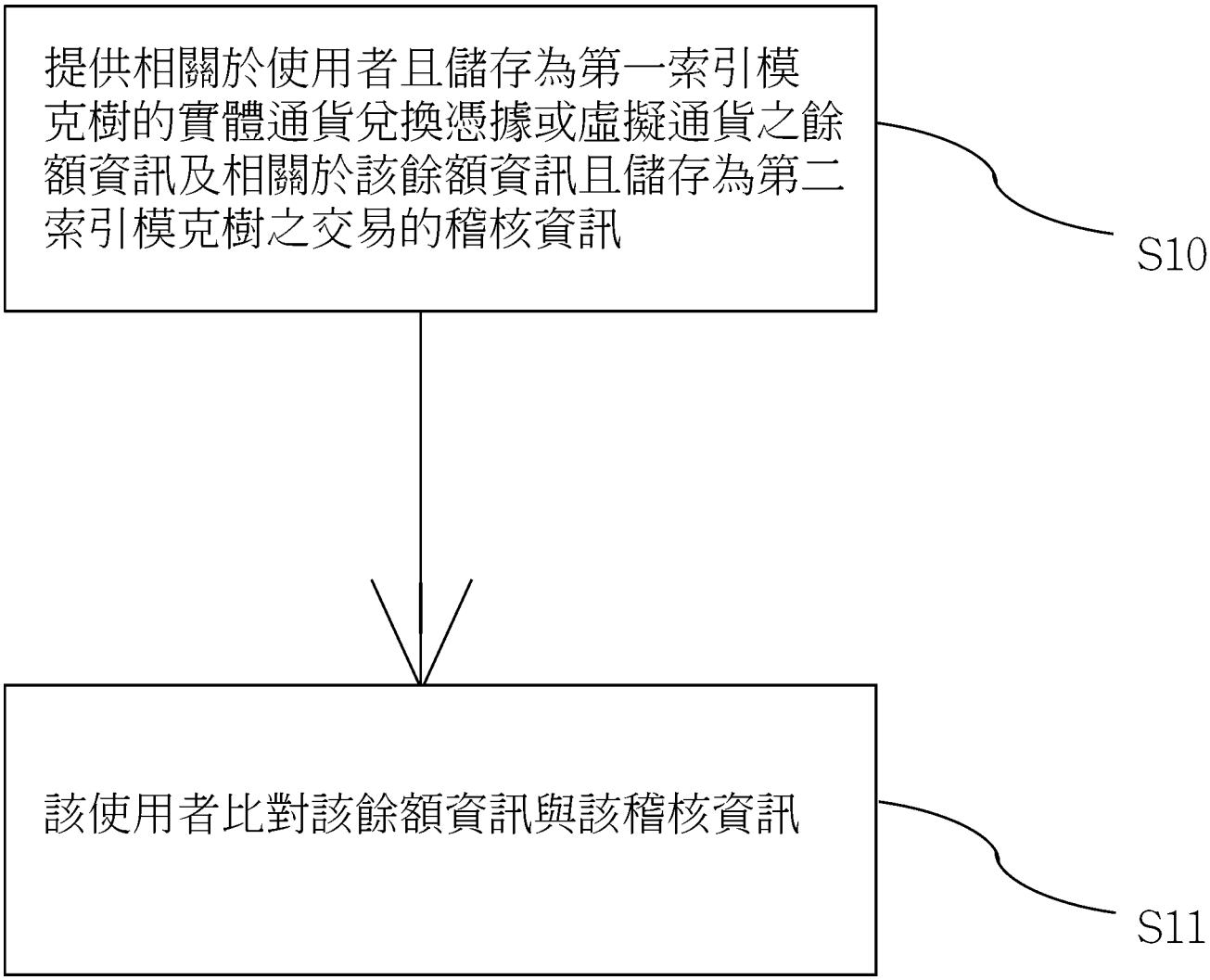
提供相關於使用者且儲存為第一索引模克樹的實體通貨兌換憑據或虛擬通貨之餘額資訊及相關於該餘額資訊且儲存為第二索引模克樹之交易的稽核資訊
S10
該使用者比對該餘額資訊與該稽核資訊
S11

圖1

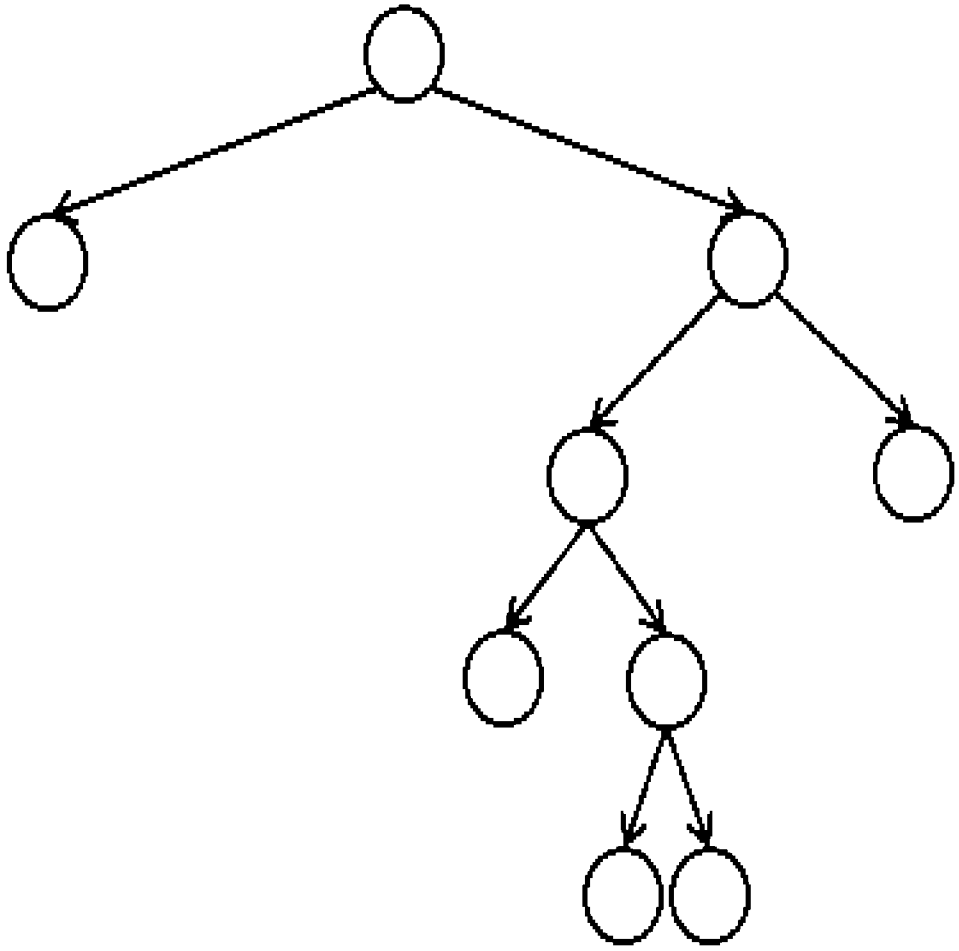

圖2

合約

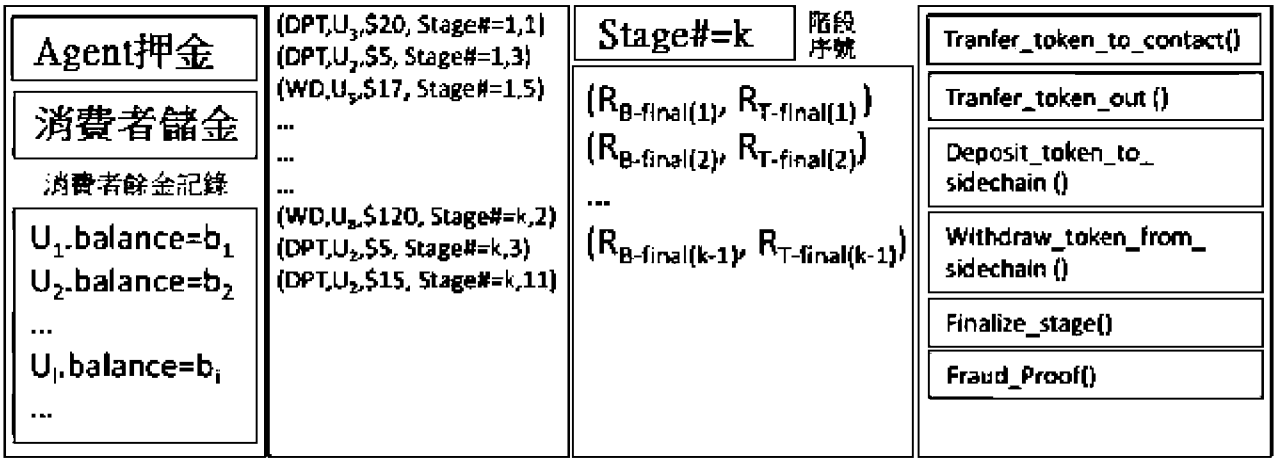
Agent押金
消費者儲金
消費者餘金記錄
U1.balance=b1
U2.balance=b2
...
Ui.balance=bi
...
(DPT,U3,$20, Stage#=1,1)
(DPT,U7,$5, Stage#=1,3)
(WD,U5,$17, Stage#=1,5)
...
...
...
(WD,Un,$120, Stage#=k,2)
(DPT,U2,$5, Stage#=k,3)
(DPT,U2,$15, Stage#=k,11)
Stage#=k
階段序號
(RB-final(1), RT-final(1))
(RB-final(2), RT-final(2))
...
(RB-final(k-1), RT-final(k-1))
Tranfer_token_to_contact()
Tranfer_token_out ()
Deposit_token_to_sidechain ()
Withdraw_token_from_sidechain ()
Finalize_stage()
Fraud_Proof()
金庫及參與者合約餘金記錄
合約及索引模克樹金流記錄
階段狀態值
合約函式

圖3

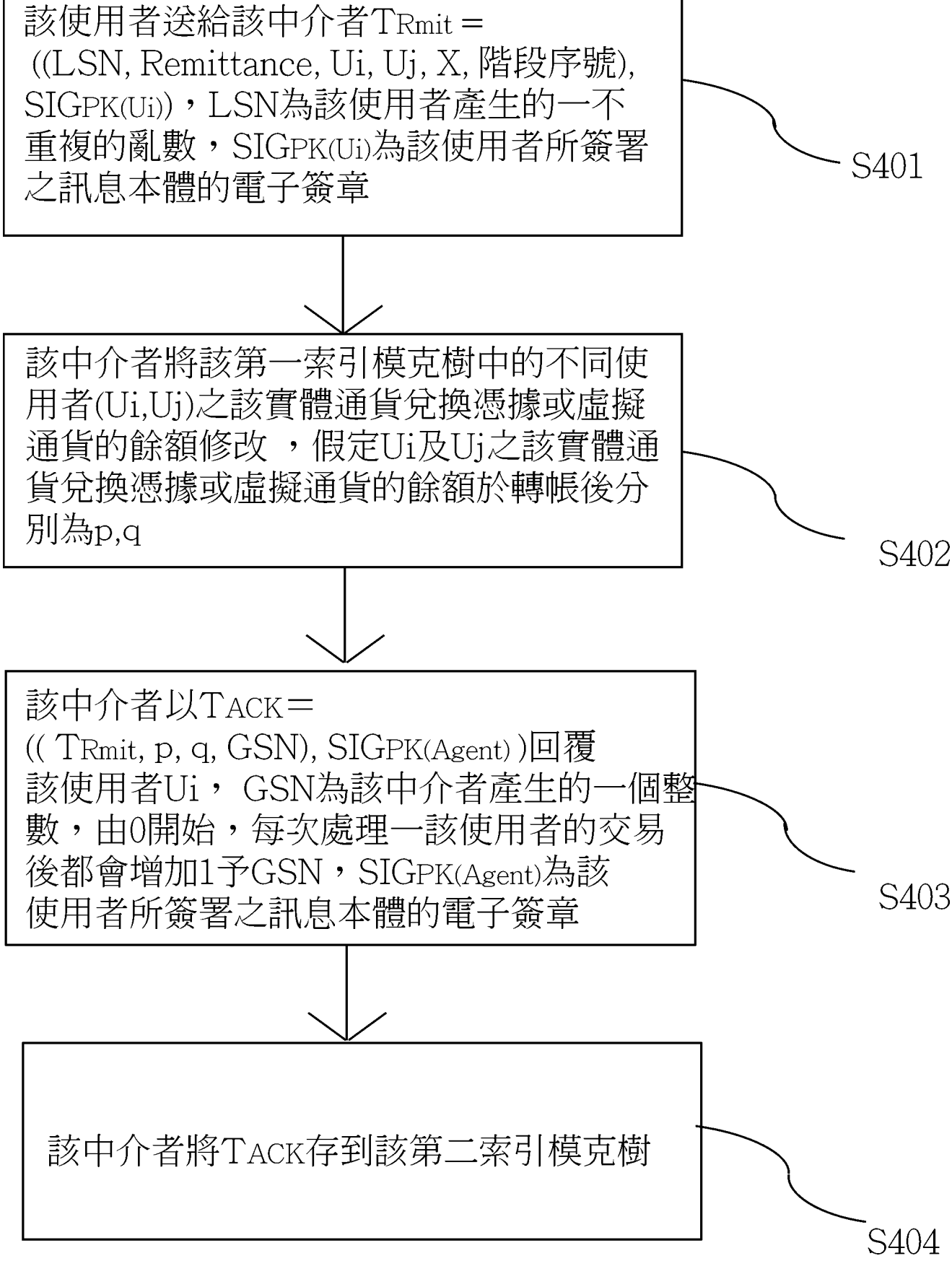
該使用者送給該中介者TRmit＝((LSN, Remittance, Ui, Uj, X, 階段序號), SIGPK(Ui))，LSN為該使用者產生的一不重複的亂數，SIGPK(Ui)為該使用者所簽署之訊息本體的電子簽章
S401
該中介者將該第一索引模克樹中的不同使用者(Ui,Uj)之該實體通貨兌換憑據或虛擬通貨的餘額修改 ，假定Ui及Uj之該實體通貨兌換憑據或虛擬通貨的餘額於轉帳後分別為p,q
S402
該中介者以TACK＝((TRmit, p, q, GSN), SIGPK(Agent))回覆該使用者Ui， GSN為該中介者產生的一個整數，由0開始，每次處理一該使用者的交易後都會增加1予GSN，SIGPK(Agent)為該使用者所簽署之訊息本體的電子簽章
S403
該中介者將TACK存到該第二索引模克樹
S404

圖4

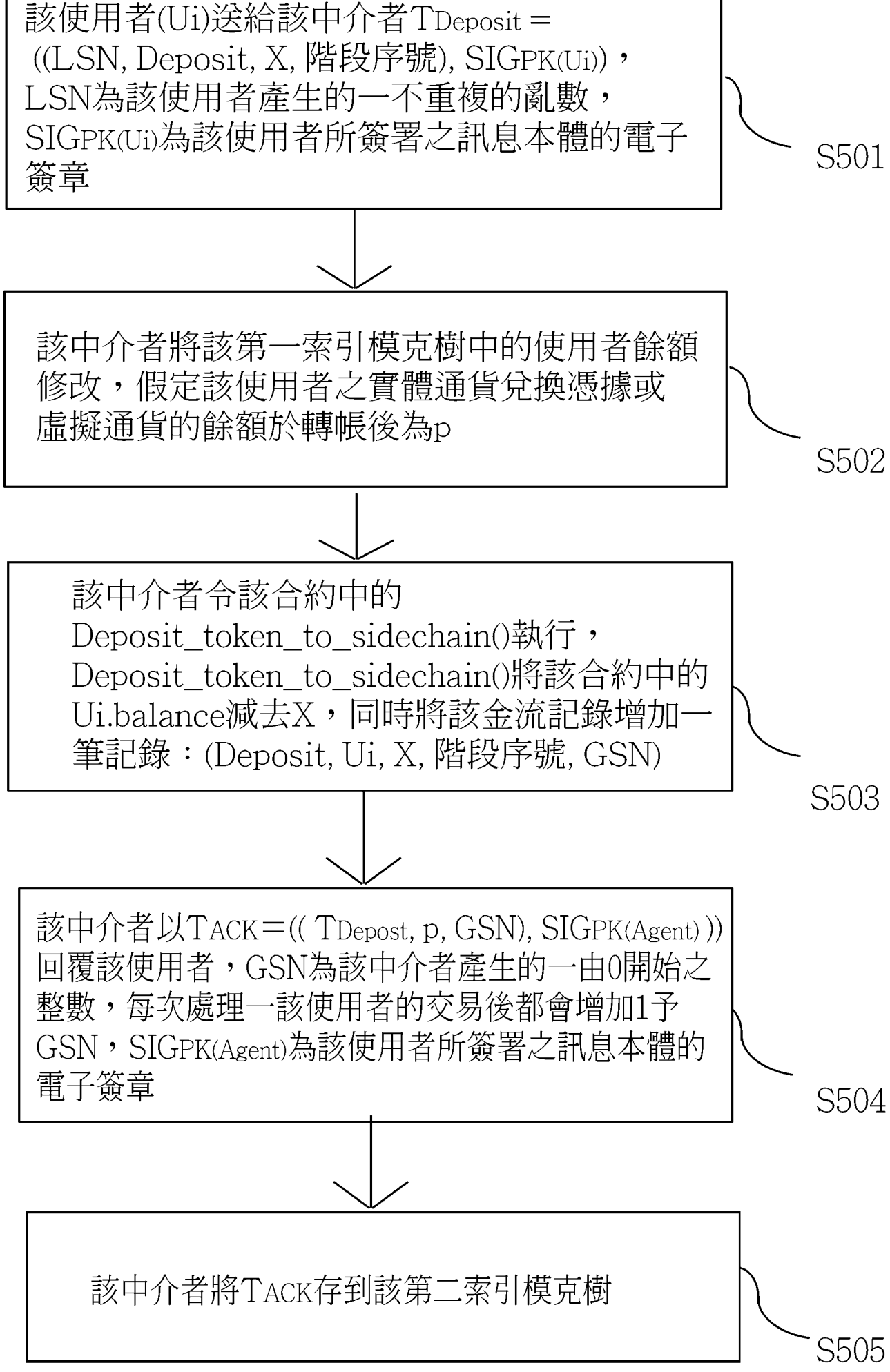
該使用者(Ui)送給該中介者TDeposit＝((LSN, Deposit, X, 階段序號), SIGPK(Ui))，LSN為該使用者產生的一不重複的亂數，SIGPK(Ui)為該使用者所簽署之訊息本體的電子簽章
S501
該中介者將該第一索引模克樹中的使用者餘額修改，假定該使用者之實體通貨兌換憑據或虛擬通貨的餘額於轉帳後為p
S502
該中介者令該合約中的Deposit_token_to_sidechain()執行，Deposit_token_to_sidechain()將該合約中的Ui.balance減去X，同時將該金流記錄增加一筆記錄：(Deposit, Ui, X, 階段序號, GSN)
S503
該中介者以TACK＝((TDepost, p, GSN), SIGPK(Agent)))回覆該使用者，GSN為該中介者產生的一由0開始之整數，每次處理一該使用者的交易後都會增加1予GSN，SIGPK(Agent)為該使用者所簽署之訊息本體的電子簽章
S504
該中介者將TACK存到該第二索引模克樹
S505

圖5

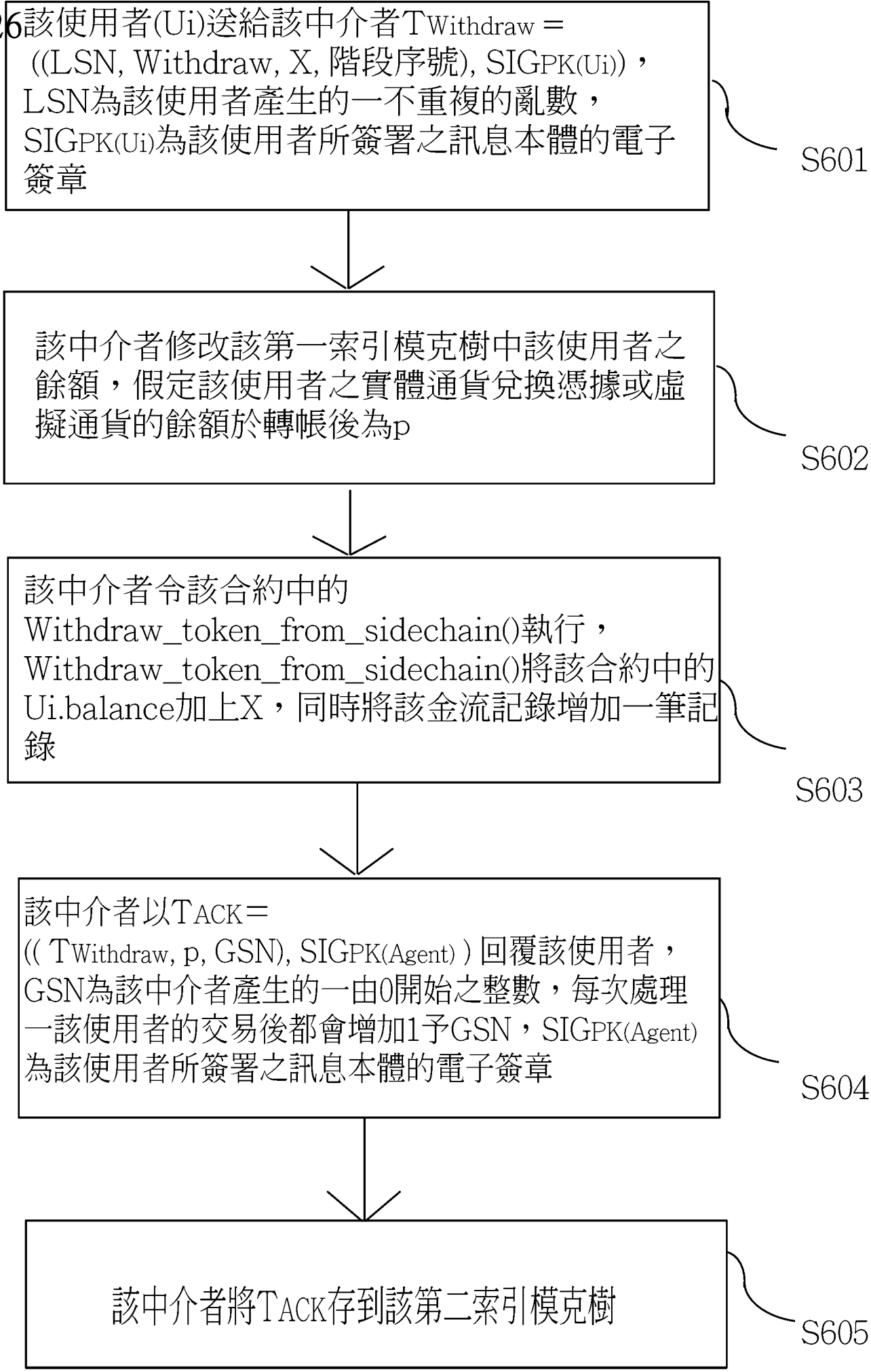
該使用者(Ui)送給該中介者TWithdraw＝((LSN, Withdraw, X, 階段序號), SIGPK(Ui))，LSN為該使用者產生的一不重複的亂數，SIGPK(Ui)為該使用者所簽署之訊息本體的電子簽章
S601
該中介者修改該第一索引模克樹中該使用者之餘額，假定該使用者之實體通貨兌換憑據或虛擬通貨的餘額於轉帳後為p
S602
該中介者令該合約中的Withdraw_token_from_sidechain()執行，Withdraw_token_from_sidechain()將該合約中的Ui.balance加上X，同時將該金流記錄增加一筆記錄
S603
該中介者以TACK＝((TWithdraw, p, GSN), SIGPK(Agent))回覆該使用者，GSN為該中介者產生的一由0開始之整數，每次處理一該使用者的交易後都會增加1予GSN，SIGPK(Agent)為該使用者所簽署之訊息本體的電子簽章
S604
該中介者將TACK存到該第二索引模克樹
S605

圖6

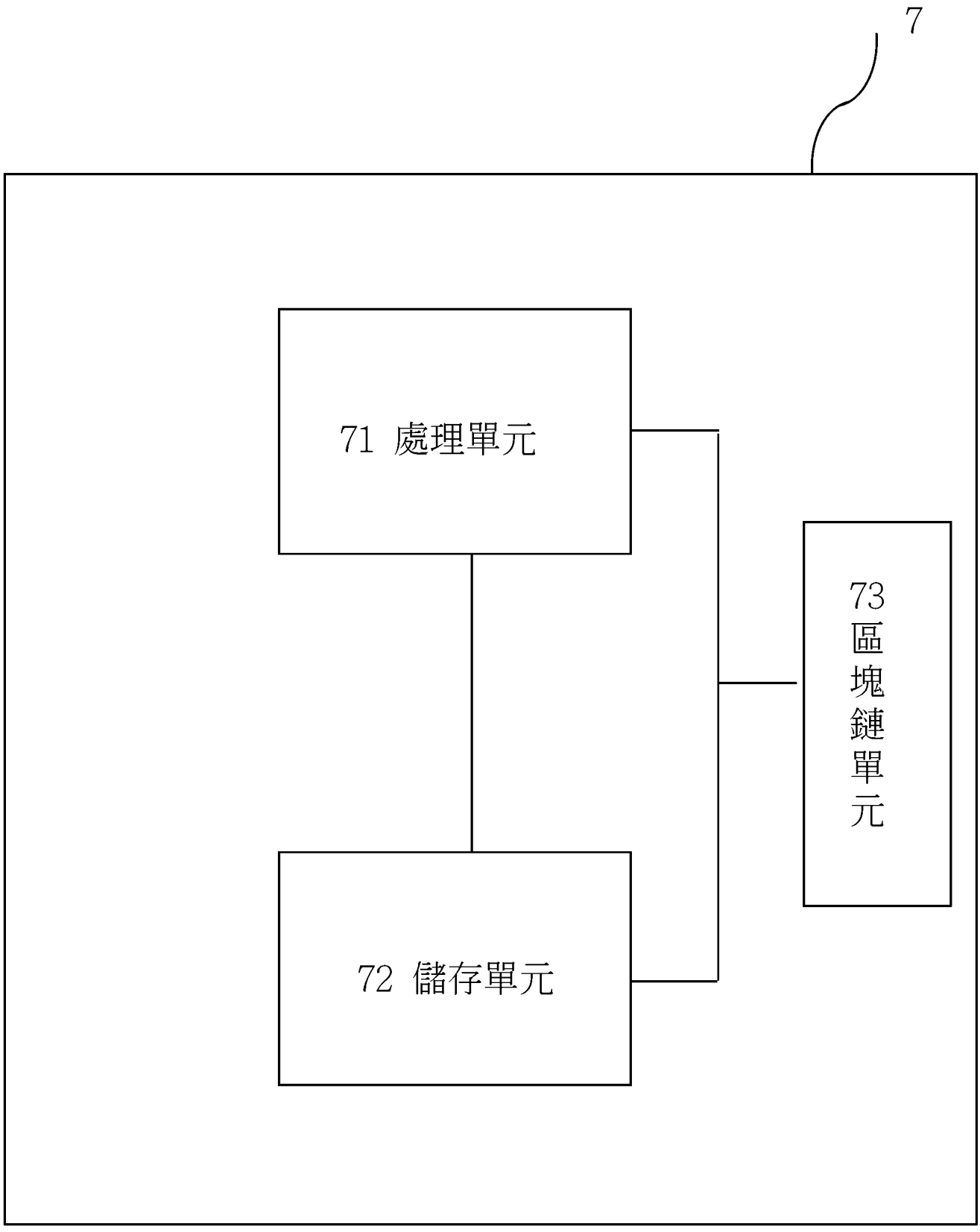

圖7

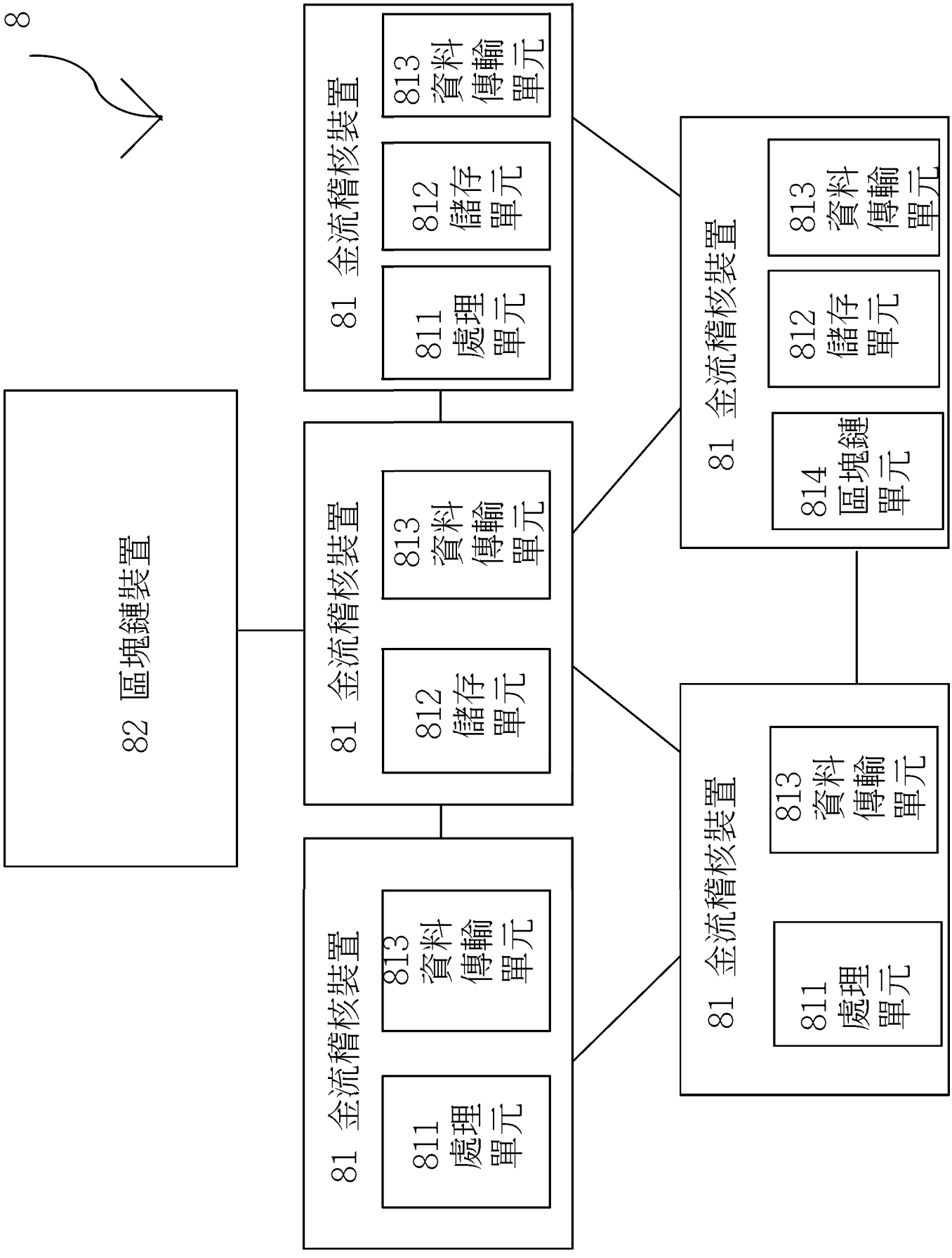
8
82 區塊鏈裝置
81 金流稽核裝置
811 處理單元
812 儲存單元
813 資料傳輸單元
81 金流稽核裝置
811 處理單元
812 儲存單元
813 資料傳輸單元
81 金流稽核裝置
811 處理單元
812 儲存單元
813 資料傳輸單元
814 區塊鏈單元
81 金流稽核裝置
811 處理單元
812 儲存單元
813 資料傳輸單元

圖8

且高效率之系統。並且，本發明能支援實體通貨兌換憑據或虛擬通貨的一般性微支付。

【圖式簡單說明】

【0044】 圖1係本發明分散式金流稽核方法之流程圖。

圖2係切片之示意圖。

圖3係本發明之合約內容的方塊圖。

圖4係本發明之轉帳交易的流程圖。

圖5係本發明之入金交易的流程圖。

圖6係本發明之出金交易的流程圖。

圖7係本發明之一種分散式金流稽核裝置的方塊圖。

圖8係本發明之一種分散式金流稽核系統的方塊圖。

【實施方式】

【0045】 為充分瞭解本發明之目的、特徵及功效，茲藉由下述具體之實施例，並配合所附之圖式，對本發明做一詳細說明，說明如後：

【0046】 請參考圖1，係本發明分散式金流稽核方法之流程圖，其步驟包括步驟S10至步驟S11。步驟S10中，其可提供相關於使用者且儲存為第一索引模克樹的實體通貨兌換憑據或虛擬通貨之餘額資訊及相關於該餘額資訊且儲存為第二索引模克樹之交易的稽核資訊。其中，第一索引模克樹及第二索引模克樹可為完滿二元雜湊樹(Full Hash Binary Tree)與指標函數Γ(Index function, 即Γ(FileName)=SHA-256(FileName) mod 2^{N-1}) 之結合。惟於其他實施例中，並不限於利用其他雜湊樹。該稽核資訊可相關於使用者，特定而言，可為複數個使用者。其中，該稽核資訊譬如一帳本，紀錄使用者之交易紀錄。於不同實施例中，